USRobotics®

Professional Access Point Administrator Guide

R46.1224.00
rev 2.0 07/06

Professional Access Point Administrator Guide

U.S. Robotics Corporation
935 National Parkway
Schaumburg, Illinois
60173-5157
USA

Contents

Getting Started

Web User Interface

Command Line Interface

Troubleshooting

About This Document

This guide describes setup, configuration, administration and maintenance of one or more Professional Access Points on a wireless network.

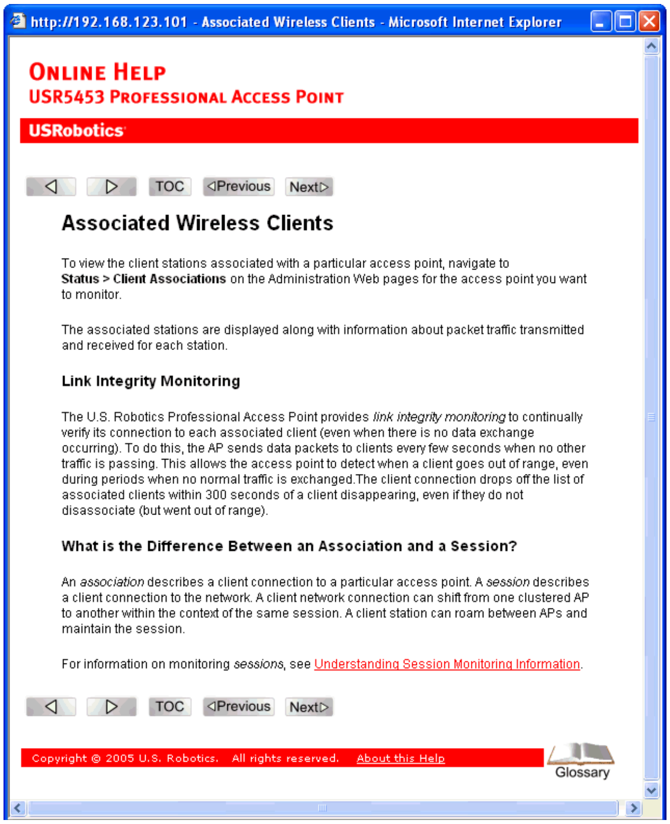
Administrator Audience

This information is intended for the person responsible for installing, configuring, monitoring, and maintaining the Professional Access Point as part of a small-to-medium business information technology infrastructure.

Online Help Features

Online Help for the Professional Access Point Web User Interface provides information about all fields and features available in the interface. The information in the Online Help is a subset of the information available in the *Administrator Guide*.

Online Help information corresponds to each tab on the Professional Access Point Web User Interface. To display help for the current tab, Click **Help** at the top of the Web User Interface page or click the **More...** link at the bottom of the tab's inline help panel.



http://192.168.123.101 - Associated Wireless Clients - Microsoft Internet Explorer
ONLINE HELP
USR5453 PROFESSIONAL ACCESS POINT
USRobotics
◁ ▷ TOC ◁Previous Next▷

Associated Wireless Clients

To view the client stations associated with a particular access point, navigate to **Status > Client Associations** on the Administration Web pages for the access point you want to monitor.

The associated stations are displayed along with information about packet traffic transmitted and received for each station.

Link Integrity Monitoring

The U.S. Robotics Professional Access Point provides *link integrity monitoring* to continually verify its connection to each associated client (even when there is no data exchange occurring). To do this, the AP sends data packets to clients every few seconds when no other traffic is passing. This allows the access point to detect when a client goes out of range, even during periods when no normal traffic is exchanged.The client connection drops off the list of associated clients within 300 seconds of a client disappearing, even if they do not disassociate (but went out of range).

What is the Difference Between an Association and a Session?

An *association* describes a client connection to a particular access point. A *session* describes a client connection to the network. A client network connection can shift from one clustered AP to another within the context of the same session. A client station can roam between APs and maintain the session.

For information on monitoring *sessions*, see Understanding Session Monitoring Information.

◁ ▷ TOC ◁Previous Next▷
Copyright © 2005 U.S. Robotics. All rights reserved. About this Help
Glossary

Recommended Settings, Notes and Cautions

An arrow next to field description information indicates a recommended or suggested configuration setting for an option on the Access Point.

A **Note** provides more information about a feature or technology and cross-references to related topics.

A **Caution** provides information about critical aspects of access point configuration, combinations of settings, events, or procedures that can adversely affect network connectivity, security, and so on.

Typographical Conventions

This guide uses the following typographical conventions:

italics	Glossary terms, new terms, and book titles
`typewriter font`	Screen text, URLs, IP addresses, and MAC addresses, UNIX file, command, and directory names, user-typed command-line entries
`typewriter font italics`	Variables
Bold Keywords	Menu titles, window names, and button names

PDF Links

In addition to URL links, which are shown in blue and underscored, this document contains links to related sections and to glossary terms. Whenever your cursor turns into the pointing hand, a single click will take you to the referenced topic.

Getting Started

This part of the Professional Access Point Administrator Guide provides the information that you need to establish a network by performing basic installation for one or more Professional Access Points:

- Overview
- Pre-Launch Checklist: Default Settings and Supported Administrator/Client Platforms
- Setting Up and Launching Your Wireless Network

Overview

The Professional Access Point provides continuous, high-speed access between your wireless and Ethernet devices. It is an advanced, standards-based solution for wireless networking in small and medium-sized businesses. The Professional Access Point enables zero-administration wireless local area network (WLAN) deployment while providing state-of-the-art wireless networking features.

The Professional Access Point provides best-of-breed security, ease-of-administration, and industry standards—providing a standalone and fully-secured wireless network without the need for additional management and security server software.

The access point can broadcast in the following modes.

- IEEE 802.11b
- IEEE 802.11g

The following sections list features and benefits of the Professional Access Point, and tell you what’s next when you’re ready to get started.

- Features and Benefits
    - IEEE Standards Support and Wi-Fi Compliance
    - Wireless Features
    - Security Features
    - Guest Interface
    - Clustering and Auto-Management
    - Networking

  - Maintainability

- What's Next?

Features and Benefits

IEEE Standards Support and Wi-Fi Compliance

- Support for IEEE 802.11b and IEEE 802.11g wireless networking standards
- Provides bandwidth of up to 11 Mbps for IEEE 802.11b and 54 Mbps for IEEE 802.11g
- Wi-Fi compliance required for certification

Wireless Features

- Auto channel selection at startup
- Transmit power adjustment
- Wireless Distribution System (WDS) for connecting multiple access points wirelessly. Extends your network with less cabling and provides a seamless experience for roaming clients.
- Quality of Service (QoS) for enhanced throughput and better performance of time-sensitive wireless traffic like Video, Audio, Voice over IP (VoIP) and streaming media. The Professional Access Point QoS is Wi-Fi Multimedia (WMM) compliant.
- Load Balancing
- Built-in support for multiple SSIDs (network names) and multiple BSSIDs (basic service set IDs) on the same access point
- Channel management for automatic coordination of radio channel assignments to reduce access-point-to-access-point interference on the network and maximise Wi-Fi bandwidth
- Neighbouring access point detection finds nearby access points, including rogues.
- Support for multiple IEEE 802.11d Regulatory Domains (country codes for global operation)

Security Features

- Prohibit SSID Broadcast
- Station isolation
- Weak IV avoidance
- Wireless Equivalent Privacy (WEP)

- Wi-Fi Protected Access 2 (WPA2/802.11i)
- Advanced Encryption Standard (AES)
- User-based access control, local user database, and user life-cycle management with built-in RADIUS authentication server
- WPA/WPA2 Enterprise
- MAC address filtering

Guest Interface

- Captive portal to guide guests to customized, guest-only Web page
- Implementation with dedicated access point or as VLAN with unique network name (SSID)

Clustering and Auto-Management

- Automatic setup with the Professional Access Point Detection Utility
- Provisioning and auto-configuration of access points through clustering and cluster rendezvous

  The administrator can specify how new access points should be configured before they are added to the network. When new access points are added to the same wired network, they can automatically rendezvous with the cluster and securely download the correct configuration. The process does not require manual intervention, but is under the control of the administrator.
- Single universal view of clustered access points and cluster configuration settings

  Configuration for all access points in a cluster can be managed from a single interface. Changes to common parameters are automatically reflected in all members of the cluster.
- Self-managed access points with automatic configuration synchronization

  The access points in a cluster periodically ensure that the cluster configuration is consistent, and check for the presence and availability of the other members of the cluster. The administrator can monitor this information through the Web User Interface.
- Enhanced local authentication using 802.1x without additional IT setup

  A cluster can maintain a user authentication server and database stored on the access points. This eliminates the need to install, configure, and maintain a RADIUS infrastructure and simplifies the administrative task of deploying a secure wireless network.

Networking

- Dynamic Host Configuration Protocol (DHCP) support for dynamically assigning network configuration information to systems on the LAN/WLAN.

- Virtual Local Area Network (VLAN) support

SNMP Support

The Professional Access Point includes the following standard Simple Network Protocol (SNMP) Management Information Bases (MIB):

- SNMP v1 and v2 MIBs
- IEEE802.11 MIB
- Four USRobotics proprietary MIBs support product, system, channel, and wireless system statistics.

Maintainability

- Status, monitoring, and tracking views of the network including session monitoring, client associations, transmit/receive statistics, and event log
- Link integrity monitoring to continually verify connection to the client, regardless of network traffic activity levels
- Reset configuration option
- Firmware upgrade
- Backup and restore of access point configuration
- Backup and restore of user database for built-in RADIUS server (when using IEEE 802.1x or WPA/ WPA2 Enterprise (RADIUS) security mode)

What’s Next?

Are you ready to get started with wireless networking? Read through the “Pre-Launch Checklist: Default Settings and Supported Administrator/Client Platforms” on page 15, and then follow the steps in “Setting Up and Launching Your Wireless Network” on page 23.

Pre-Launch Checklist: Default Settings and Supported Administrator/Client Platforms

Before you plug in and boot a new Access Point, review the following sections for hardware, software, and client configuration requirements and for compatibility issues. Make sure that you have everything you need for a successful launch and test of your new or extended wireless network.

- Professional Access Point
  - Default Settings for the Professional Access Point
  - What the Access Point Does Not Provide
- Administrator's Computer
- Wireless Client Computers
- Understanding Dynamic and Static IP Addressing on the Professional Access Point
  - How Does the Access Point Obtain an IP Address at Startup?
  - Dynamic IP Addressing
  - Static IP Addressing

Professional Access Point

The Professional Access Point provides continuous, high-speed access between your wireless and Ethernet devices in IEEE 802.11b and 802.11g modes.

The Professional Access Point offers a *Guest Interface* feature that allows you to configure access points for controlled guest access to the wireless network. This can be accomplished by using Virtual LANs. For more information on the Guest interface, see “Guest Login” on page 121 and “A Note About Setting Up Connections for a Guest Network” on page 25.

Default Settings for the Professional Access Point

Option	Default Settings	Related Information
System Name	`USR5453-AP`	"Setting the DNS Name" on page 91 in "Ethernet (Wired) Settings" on page 89
User Name	`admin` The user name is read-only. It cannot be modified.	
Password	`admin`	"Provide Administrator Password and Wireless Network Name" on page 38 in "Basic Settings" on page 35
Network Name (SSID)	`USR5453 Internal Network` for the Internal interface `USR5453 Guest Network` for the Guest interface	"Review / Describe the Access Point" on page 37 in "Basic Settings" on page 35 "Configuring Internal LAN Wireless Settings" on page 99 in "Wireless Settings" on page 97 "Configuring Guest Network Wireless Settings" on page 100 in "Wireless Settings" on page 97
Network Time Protocol (NTP)	None	"Time Protocol" on page 161
IP Address	`192.168.1.10` The default IP address is used if you do not use a *Dynamic Host Configuration Protocol* (DHCP) server. You can assign a new static IP address through the Web User Interface. If you have a DHCP server on the network, then an IP address will be dynamically assigned by the server at access point startup.	"Understanding Dynamic and Static IP Addressing on the Professional Access Point" on page 20
Connection Type	**Dynamic Host Configuration Protocol** (DHCP) If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is to change the connection type from **DHCP** to **Static IP**. The Guest network must have a DHCP server.	"Understanding Dynamic and Static IP Addressing on the Professional Access Point" on page 20 For information on how to reconfigure the Connection Type, see "Configuring Internal Interface Ethernet Settings" on page 93.
Subnet Mask	255.255.255.0 This is determined by your network setup and DHCP server configuration.	"Ethernet (Wired) Settings" on page 89

Option	Default Settings	Related Information
Radio	**On**	“Radio” on page 129
IEEE 802.11 Mode	**802.11g**	“Radio” on page 129
802.11g Channel	**Auto**	“Radio” on page 129
Beacon Interval	**100**	“Radio” on page 129
DTIM Period	**2**	“Radio” on page 129
Fragmentation Threshold	**2346**	“Radio” on page 129
Regulatory Domain	**FCC**	“Radio” on page 129
RTS Threshold	**2347**	“Radio” on page 129
MAX Stations	**2007**	“Radio” on page 129
Transmit Power	**100 percent**	“Radio” on page 129
Rate Sets Supported (Mbps)	• **IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1** • **IEEE 802.11b: 11, 5.5, 2, 1**	“Radio” on page 129
Rate Sets (Mbps) (Basic/Advertised)	• **IEEE 802.1g: 11, 5.5, 2, 1** • **IEEE 802.1b: 2, 1**	“Radio” on page 129
Broadcast SSID	**Allow**	“Broadcast SSID, Station Isolation, and Security Mode” on page 107 in “Security” on page 101
Security Mode	None	“Broadcast SSID, Station Isolation, and Security Mode” on page 107 in “Security” on page 101
Authentication Type	None	
MAC Filtering	**Allow any station unless in list**	“MAC Filtering” on page 135
Guest Login and Management	**Disabled**	“Guest Login” on page 121
Load Balancing	**Disabled**	“Load Balancing” on page 139
WDS Settings	None	“Wireless Distribution System” on page 153
SNMP	**Enabled**	“Enabling and Disabling Simple Network Management Protocol (SNMP)” on page 166
SNMP SET Requests	**Disabled**	“Enabling and Disabling Simple Network Management Protocol (SNMP)” on page 166

What the Access Point Does Not Provide

The Professional Access Point is not designed to function as a gateway to the Internet. To connect your Wireless LAN (WLAN) to other LANs or the Internet, you need a gateway device.

Administrator’s Computer

Configuration and administration of the Professional Access Point is accomplished with the Professional Access Point Detection Utility, which you run from the CD, and through a Web-based user interface. The following table describes the minimum requirements for the administrator’s computer.

Required Software or Component	Description
Ethernet Connection to the First Access Point	The computer used to configure the first access point with the Detection Utility must be connected to the access point, either directly or through a hub, by an Ethernet cable. For more information on this step, see “Step 2. Connect the access point to network and power” on page 24 in Setting Up and Launching Your Wireless Network.
Wireless Connection to the Network	After initial configuration and launch of the first access point on your new wireless network, you can make subsequent configuration changes through the Web User Interface using a wireless connection to the internal network. For wireless connection to the access point, your administration device needs Wi-Fi capability: • Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. IEEE 802.11b and 802.11g modes are supported. • Wireless client software such as Microsoft Windows XP or Funk Odyssey wireless client configured to associate with the Professional Access Point. For more details on Wi-Fi client setup, see “Wireless Client Computers” on page 19.
Web Browser / Operating System	Configuration and administration of the Professional Access Point is provided through a Web-based user interface hosted on the access point. USRobotics recommends using one of the following supported Web browsers to access the Web User Interface: • Microsoft Internet Explorer version 5.5 or 6.x (with up-to-date patch level for either major version) on Microsoft Windows XP or Microsoft Windows 2000 • Mozilla 1.7.x on Redhat 9 with 2.4 kernel The administration Web browser must have JavaScript enabled to support the interactive features of the Web User Interface. The browser must also support HTTP uploads to use the firmware upgrade feature.

Required Software or Component	Description
Detection Utility Wizard on CD-ROM	You can run the Installation CD-ROM on any Windows laptop or computer that is connected to the access point via wired or wireless connection. It detects Professional Access Points on the network. The wizard steps you through initial configuration of new access points, and provides a link to the Web User Interface where you finish the basic setup process in a step-by-step mode and launch the network. For more information about using the Detection Utility, see “Step 3. Run the Detection Utility to find access points on the network” on page 26 under “Setting Up and Launching Your Wireless Network”.
CD-ROM Drive	The administrator’s computer must have a CD-ROM drive to run the Installation CD-ROM.
Security Settings	Ensure that security is disabled on the wireless client used to initially configure the access point.

Wireless Client Computers

The Professional Access Point provides wireless access to any client with a properly configured Wi-Fi client adapter for the 802.11 mode in which the access point is running.

Multiple client operating systems are supported. Clients can be laptops or desktops, personal digital assistants (PDAs), or any other hand-held, portable, or stationary device equipped with a Wi-Fi adapter and supporting drivers.

In order to connect to the access point, wireless clients need the following software and hardware.

Required Component	Description
Wi-Fi Client Adapter	Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE 802.11b and 802.11g modes are supported.) Wi-Fi client adapters vary considerably. The adapter can be a PC card built in to the client device, a portable PCMCIA or PCI card, or an external device such as a USB or Ethernet adapter that you connect to the client by means of a cable. The access point supports 802.11b/g modes, but you will probably make a decision during network design phase as to which mode to use. The fundamental requirement for clients is that they all have configured adapters that match the 802.11 mode for which your access point is configured.
Wireless Client Software	Client software such as Microsoft Windows Supplicant or Funk Odyssey wireless client configured to associate with the Professional Access Point.

Required Component	Description
Client Security Settings	Security should be disabled on the client used to do initial configuration of the access point. If the Security mode on the access point is set to anything other than None, wireless clients will need to set a profile to the authentication mode used by the access point and provide a valid user name and password, certificate, or similar user identity proof. Security modes are Static WEP, IEEE 802.1x, WPA/WPA2 with RADIUS server, and WPA/WPA2-PSK. For information on configuring security on the access point, see “Security” on page 101.

Understanding Dynamic and Static IP Addressing on the Professional Access Point

Professional Access Points are designed to auto-configure, with very little setup required for the first access point and miminal configuration required for additional access points subsequently joining a preconfigured *cluster*.

How Does the Access Point Obtain an IP Address at Startup?

When you deploy the access point, it looks for a network DHCP server and, if it finds one, obtains an IP Address from the DHCP server. If no DHCP server is found on the network, the access point will continue to use its default Static IP Address (192.168.1.10) until you reassign it a new static IP address and specify a static IP addressing policy or until a DHCP server is brought online.

Note

- If you configure both an Internal and Guest network and plan to use a dynamic addressing policy for both, separate DHCP servers must be running on each network.
- A DHCP server is a requirement for the Guest network.

When you run the Detection Utility, it discovers the Professional Access Points on the network and lists their IP addresses and MAC addresses. The Detection Utility also provides a link to the Web User Interface of each access point using the IP address in the URL. For more information about the Detection Utility, see “Step 3. Run the Detection Utility to find access points on the network” on page 26.

Dynamic IP Addressing

The Professional Access Point generally expects that a DHCP server is running on the network where the access point is deployed. Most business networks already have DHCP service provided through either a gateway device or a centralized server. However, if no DHCP server is present on the Internal network, the access point will use the default Static IP Address for first-time startup.

Similarly, wireless clients and other network devices will receive their IP addresses from the DHCP server, if there is one. If no DHCP server is present on the network, you must manually assign static IP addresses to your wireless clients and other network devices.

The Guest network must have a DHCP server.

Static IP Addressing

The Professional Access Point ships with a default Static IP Address of 192.168.1.10. (See "Default Settings for the Professional Access Point" on page 16.) If no DHCP server is found on the network, the access point retains this static IP address at first-time startup.

After access point startup, you have the option of specifying a static IP addressing policy on Professional Access Points and assigning static IP addresses to APs on the Internal network via the access point Web User Interface. (See information about the **Connection Type** field and related fields in "Configuring Internal Interface Ethernet Settings" on page 93.)

Caution If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP. You can either assign a new Static IP address to the access point or continue using the default address. USRobotics recommends assigning a new Static IP address so that if later you bring up another Professional Access Point on the same network, the IP address for each access point will be unique.

Recovering an IP Address

If you experience trouble communicating with the access point, you can recover a Static IP Address by resetting the access point configuration to the factory defaults (see "Reset Configuration" on page 171), or you can get a dynamically assigned address by connecting the access point to a network that has DHCP.

Setting Up and Launching Your Wireless Network

Setting up and deploying one or more Professional Access Points is in effect creating and launching a wireless network. The Detection Utility wizard and corresponding Basic Settings Administration Web page simplify this process. Here is a step-by-step guide to setting up your Professional Access Points and the resulting wireless network. Have the Installation CD-ROM handy, and familiarise yourself with the “Pre-Launch Checklist: Default Settings and Supported Administrator/Client Platforms” on page 15 if you haven’t already. The topics covered here are:

- Step 1. Unpack the access point
- Step 2. Connect the access point to network and power
- Step 3. Run the Detection Utility to find access points on the network
- Step 4. Log on to the Web User Interface
- Step 5. Configure Basic Settings and start the wireless network
- Wall Mounting the Access Point

Step 1. Unpack the access point

Unpack the access point and familiarize yourself with its hardware ports, associated cables, and accessories.

Access Point Hardware and Ports

The Access Point includes:

- Ethernet port for connection to the Local Area Network (LAN) via Ethernet network cable
- Power port and power adapter
- Reset button
- Two 5 dB antennas

What’s inside the Access Point?

An access point is a single-purpose device designed to function as a wireless hub. Inside the access point is a Wi-Fi radio system, a microprocessor, and a mini-PC card. The access point boots from FlashROM that contains USRobotics firmware with the configurable, runtime features summarized in “Overview” on page 11.

As new features and enhancements become available, you can upgrade the firmware to add new functionality and performance improvements to the access points that make up your wireless network. (See “Upgrade” on page 172.)

Step 2. Connect the access point to network and power

The next step is to set up the network and power connections.

1. Do one of the following to create an Ethernet connection between the access point and your computer:

   - Connect one end of an Ethernet cable to the LAN port on the access point and the other end to the same networking device (such as a router) to which your computer is connected (see Figure 1).

   Or

   - Connect one end of an Ethernet cable to the LAN port on the access point and the other end of the cable to the Ethernet port on your computer (see Figure 2).

Initial Connection Notes

If you use a hub, the device that you use must permit broadcast signals from the access point to reach all other devices on the network. A standard hub should work fine. Some *switches*, however, do not allow directed or subnet broadcasts through. You may have to configure the switch to allow directed broadcasts.

For initial configuration with a direct Ethernet connection and no DHCP server, be sure to set your computer to a static IP address in the subnet 255.255.255.0. (The default IP address for the access point is 192.168.1.10.)

If for initial configuration you use a direct Ethernet (wired) connection between the access point and your computer, you will need to reconfigure the cabling for subsequent startup and deployment of the access point so that the access point is no longer connected directly to your computer but instead is connected to the LAN (either via a networking device as shown in Figure 1 or directly).

It is possible to detect access points on the network (using the Detection Utility) with a wireless connection. However, USRobotics strongly advises against using this method. In your environment you may have no way of knowing whether you are connecting to the intended access point, and the initial configuration changes required may cause you to lose connectivity with the access point over a wireless connection.

Figure 1. Ethernet Connections When Using DHCP for Initial Configuration.

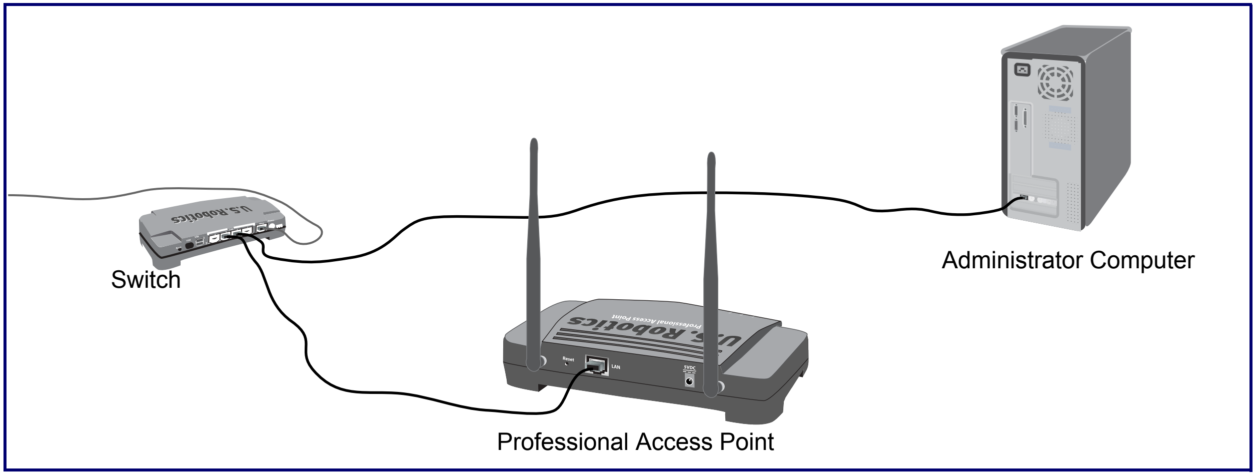
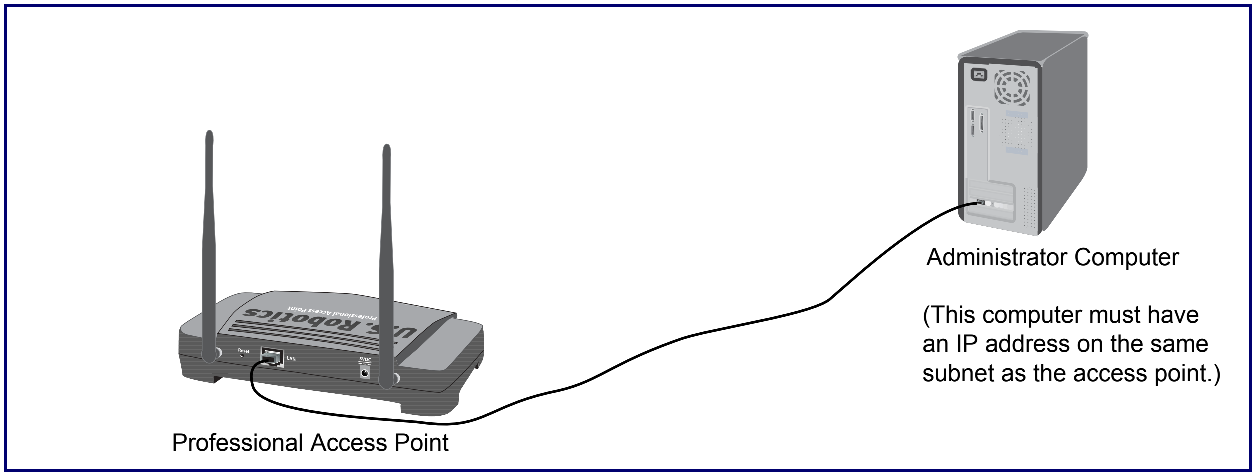


Figure 2. Ethernet Connections When Using Static IP Address for Initial Configuration.


Administrator Computer
(This computer must have
an IP address on the same
subnet as the access point.)
U.S.Robotics
Professional Access Point

2. Connect the power adapter to the power port on the back of the access point, and then plug the other end of the power adapter into a power outlet (preferably, via a surge protector).

Note to UK Users Replace the plug on the power adapter with the UK standard plug that is supplied in your USRobotics package. Apply enough pressure to cause a click and firmly seat the new plug in the adapter.

Note The access point may take up to one minute to boot. To ensure a smooth installation process, USRobotics recommends that you wait one minute before proceeding with “Step 3. Run the Detection Utility to find access points on the network”.

A Note About Setting Up Connections for a Guest Network

The Professional Access Point offers a Guest Interface that allows you to configure an access point for controlled guest access to the network. The same access point can function as a bridge for two different wireless networks: a secure Internal LAN and a public Guest network. This can be done virtually, by defining two different Virtual LANs in the Web User Interface.

Hardware Connections for a Guest VLAN

If you plan to configure a guest network using VLANs, do the following:

- Connect the LAN port on the access point to a VLAN-capable switch.
- Define VLANs on that switch.

Once you have the required physical connections set up, the rest of the configuration process is accomplished through the Web User Interface. For information on configuring Guest interface settings in the Web User Interface, see “Guest Login” on page 121.

If you plan to configure the access point for guest access only, without maintaining separate Internal and Guest networks, you do not need a VLAN-capable switch.

Step 3. Run the Detection Utility to find access points on the network

The Detection Utility is an easy-to-use utility for discovering and identifying new Professional Access Points. The Detection Utility scans the network looking for access points, and displays ID details on those it finds.

Notes and Cautions

- Keep in mind that the Detection Utility recognizes and configures only USRobotics Professional Access Points. The Detection Utility will not find any other devices.
- Run the Detection Utility only in the subnet of the internal network (SSID). Do not run the Detection Utility on the guest subnetwork.
- The Detection Utility will find only those access points that have IP addresses. IP addresses are dynamically assigned to APs if you have a DHCP server running on the network. Keep in mind that if you deploy the access point on a network with no DHCP server, the default static IP address (192.168.1.10) will be used.

  Use caution with non-DHCP enabled networks: Do not deploy more than one new access point on a non-DHCP network because they will use the same default static IP addresses and conflict with each other. (For more information, see “Understanding Dynamic and Static IP Addressing on the Professional Access Point” on page 20 and “How Does the Access Point Obtain an IP Address at Startup?” on page 20.)

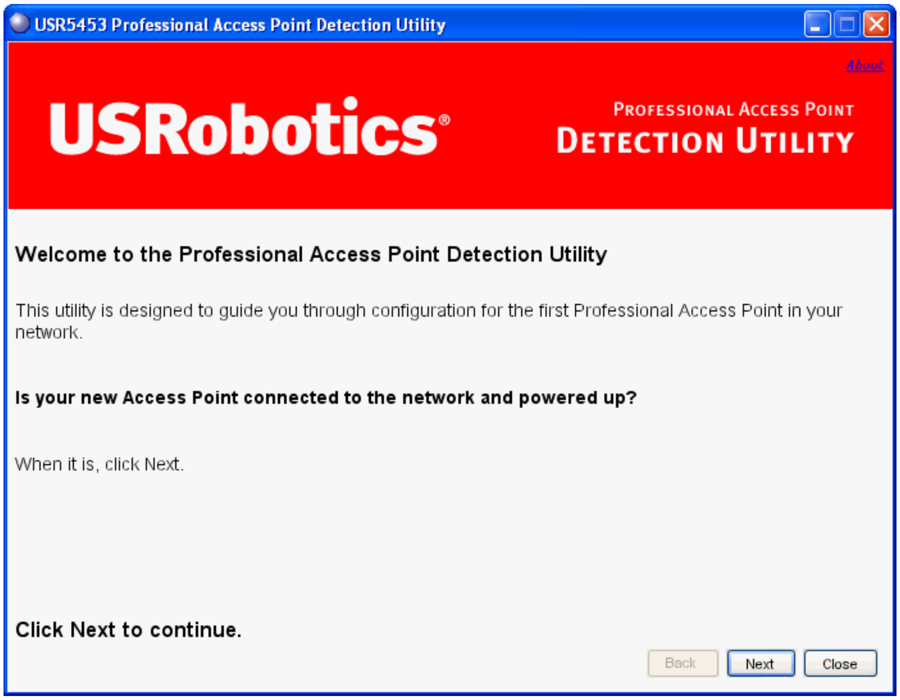
Run the Installation CD-ROM on a laptop or computer that is connected to the same network as your access points and use it to step through the discovery process as follows:

1. Insert the Installation CD-ROM into the CD-ROM drive on your computer and select **Setup** from the menu.

   If the CD-ROM does not start automatically, navigate to the CD-ROM drive and double-click **setup.exe**.

   If you receive a Windows Security Alert from your Windows Firewall, click **Unblock** to enable the java program to access your network. If network access is blocked, the Detection Utility cannot find your access point.

The Detection Utility Welcome screen is displayed.


USR5453 Professional Access Point Detection Utility
About
USRobotics®
Professional Access Point
Detection Utility

Welcome to the Professional Access Point Detection Utility

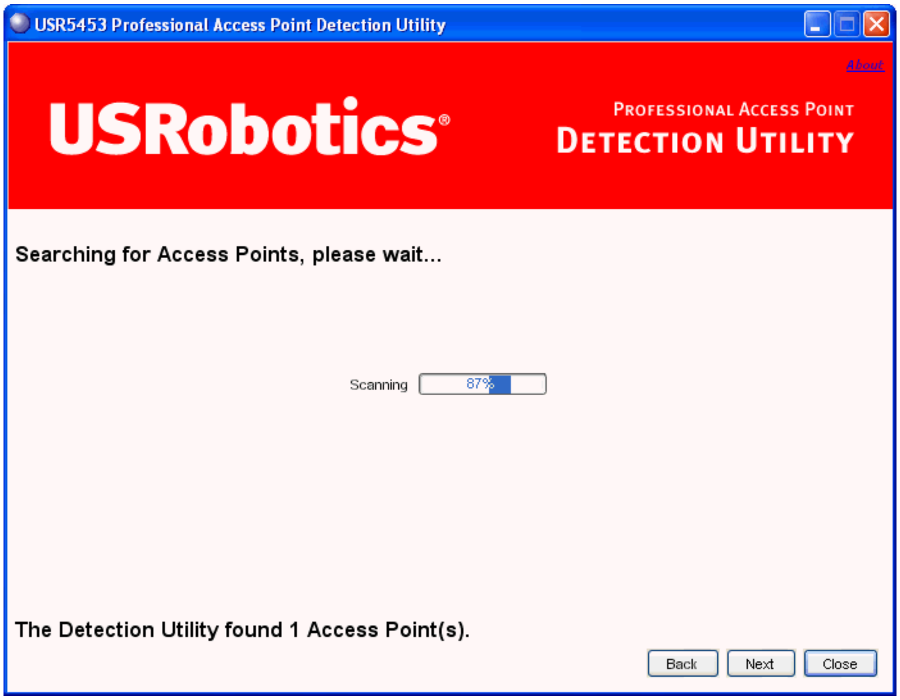
This utility is designed to guide you through configuration for the first Professional Access Point in your network.

Is your new Access Point connected to the network and powered up?

When it is, click Next.

Click Next to continue.

2. Click **Next** to search for access points. Wait for the search to complete, or until the Detection Utility has found your new access points.


USR5453 Professional Access Point Detection Utility
About
USRobotics®
Professional Access Point
Detection Utility
Scanning
87%
Back
Next
Close

Searching for Access Points, please wait...

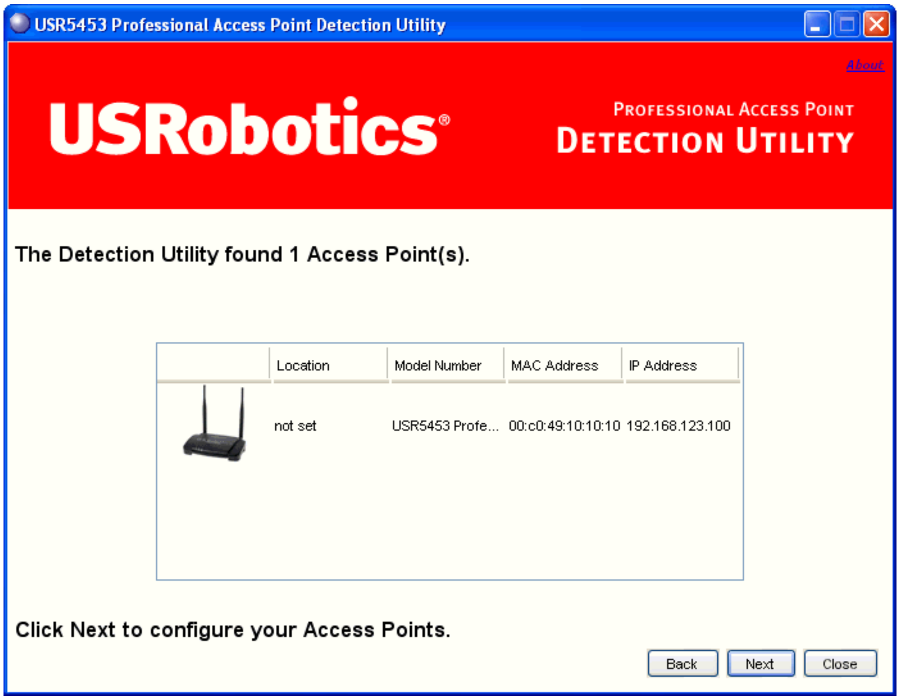
The Detection Utility found 1 Access Point(s).

Note If no access points are found, the Detection Utility indicates this and presents troubleshooting information about your LAN and power connections. Once you have checked hardware power and Ethernet connections, you can click the Detection Utility **Back** button to search again for access points.

3. Review the list of access points found.

   The Detection Utility will detect the IP addresses of Professional Access Points. Access points are listed with their locations,MAC addresses, and IP Addresses. If you are installing the first access point on a single-access-point network, only one entry will be displayed on this screen

   Verify the MAC addresses shown here against the Professional Access Point’s LAN MAC address. (You can find the LAN MAC on the label on the bottom of the access point.) This will be especially helpful later in providing or modifying the descriptive **Location** name for each access point.


USR5453 Professional Access Point Detection Utility
About
USRobotics
Professional Access Point
Detection Utility
Back
Next
Close

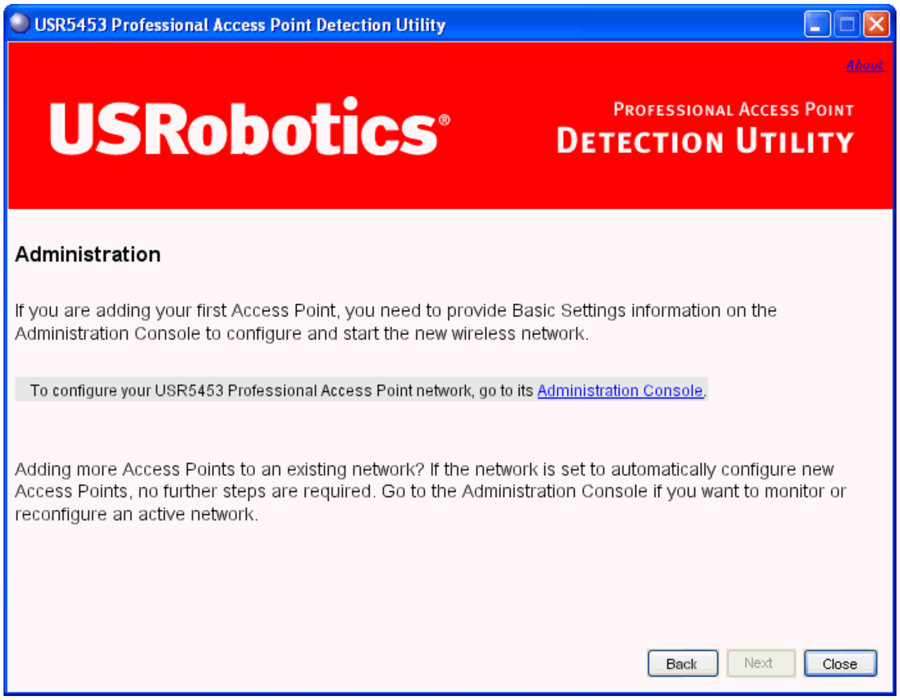
The Detection Utility found 1 Access Point(s).

	Location	Model Number	MAC Address	IP Address
	not set	USR5453 Profe...	00:c0:49:10:10:10	192.168.123.100

Click Next to configure your Access Points.

Click **Next**.

4. Go to the Access Point Web User Interface by clicking the link provided on the Detection Utility page.


USR5453 Professional Access Point Detection Utility
About
USRobotics
Professional Access Point
Detection Utility
Back
Next
Close

Administration

If you are adding your first Access Point, you need to provide Basic Settings information on the Administration Console to configure and start the new wireless network.

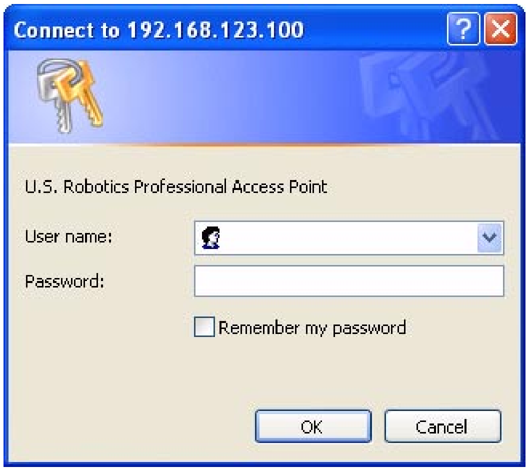
To configure your USR5453 Professional Access Point network, go to its Administration Console.

Adding more Access Points to an existing network? If the network is set to automatically configure new Access Points, no further steps are required. Go to the Administration Console if you want to monitor or reconfigure an active network.

Note The Detection Utility provides a link to the Web User Interface via the IP address of the *first* Professional Access Point.The Web User Interface is a management tool that you can access via the IP address for any access point in a cluster. (For more information about clustering see “Understanding Clustering” on page 44.)

Step 4. Log on to the Web User Interface

When you follow the link from the Detection Utility to the Professional Access Point Web User Interface, you are prompted for a user name and password.



Connect to 192.168.123.100

U.S. Robotics Professional Access Point

User name:

Password:

□ Remember my password

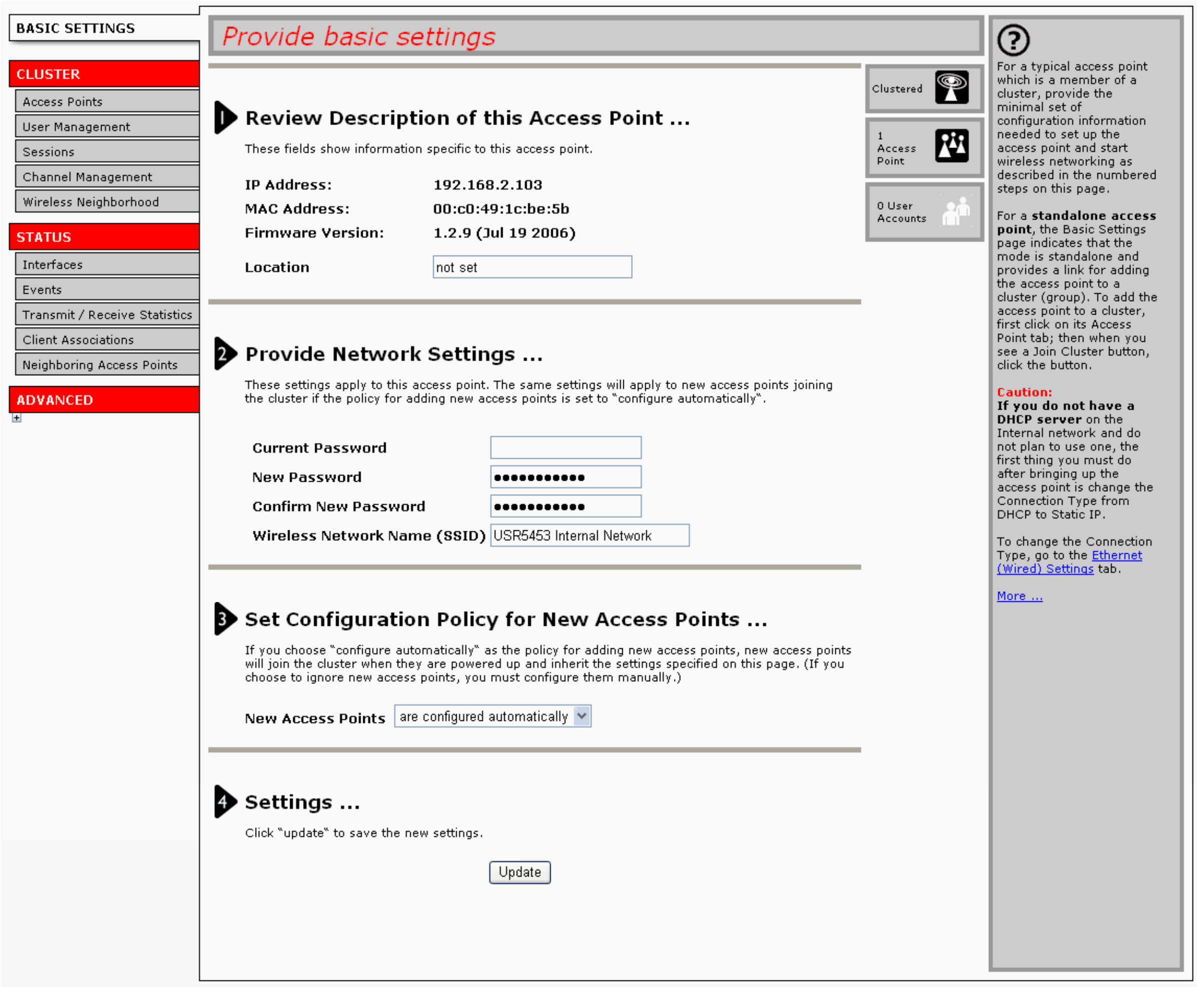
The defaults for user name and password are as follows.

Field	Default Setting
Username	admin
Password	admin

Enter the user name and password and click **OK**.

Viewing Basic Settings for Access Points

When you first log in, the Basic Settings page for Professional Access Point administration is displayed. These are global settings for all access points that are members of the cluster and, if automatic configuration is specified, for any new access points that are added later.



Provide basic settings

1 Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address:	192.168.2.103
MAC Address:	00:c0:49:1c:be:5b
Firmware Version:	1.2.9 (Jul 19 2006)
Location	not set

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

Current Password	
New Password	●●●●●●●●●●●●
Confirm New Password	●●●●●●●●●●●●
Wireless Network Name (SSID)	USR5453 Internal Network

3 Set Configuration Policy for New Access Points ...

If you choose "configure automatically" as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points: are configured automatically

4 Settings ...

Click "update" to save the new settings.

Update

For a typical access point which is a member of a cluster, provide the minimal set of configuration information needed to set up the access point and start wireless networking as described in the numbered steps on this page.

For a **standalone access point**, the Basic Settings page indicates that the mode is standalone and provides a link for adding the access point to a cluster (group). To add the access point to a cluster, first click on its Access Point tab; then when you see a Join Cluster button, click the button.

Caution:
If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

To change the Connection Type, go to the Ethernet (Wired) Settings tab.

More ...

Step 5. Configure Basic Settings and start the wireless network

Provide a minimal set of configuration information by defining the basic settings for your wireless network. These settings are all available on the Basic Settings page of the Web User Interface, and are categorized into steps 1-4 on the Web page.

For a detailed description of these Basic Settings and how to properly configure them, please see “Basic Settings” on page 35. Summarized briefly, the steps are:

1. Review Description of this Access Point.

   Provide IP addressing information. For more information, see “Review / Describe the Access Point” on page 37.

2. Provide Network Settings.

Provide a new administrator password for clustered access points. For more information, see “Provide Administrator Password and Wireless Network Name” on page 38.

3. Set Configuration Policy for New Access Points.

   Choose to configure new access points automatically (as new members of the cluster) or ignore new access points.

   If you set a configuration policy to **configure new access points automatically,** new access points added to this network will join the cluster and be configured automatically based on the settings you defined here. Updates to the **Network** settings on any cluster member will be shared with all other access points in the group.

   If you chose to **ignore new access points**, any additional access points will run in standalone mode. In standalone mode, an access point does not share the cluster configuration with other access points; it must be configured manually.

   You can always update the settings on a standalone access point to have it join the cluster. You can also remove an access point from a cluster thereby switching it to run in standalone mode.

   For more information, see “Set Configuration Policy for New Access Points” on page 39.

4. Start Wireless Networking

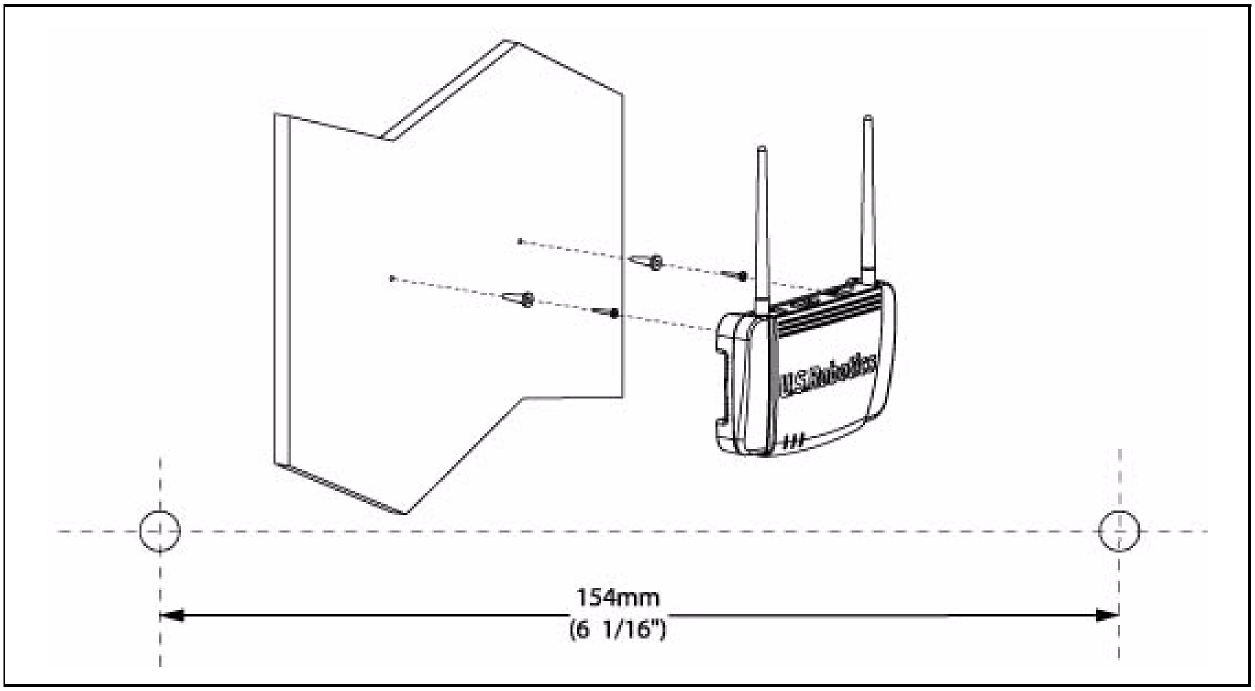
   Click the **Update** button to activate the wireless network with these new settings. For more information, see “Update Basic Settings” on page 40.

Default Configuration

If you follow the steps above and accept all the defaults, the access point will have the default configuration described in “Default Settings for the Professional Access Point” on page 16.

Wall Mounting the Access Point

The access point has keyhole openings for easy wall mounting. To expose the openings, remove the pads from the rear feet. You can then mount the access point to the wall with two anchored screws, as shown in the following illustration:



What's Next?

Next, make sure the access point is connected to the LAN, bring up your wireless clients, and connect the clients to the network. Once you have tested the basics of your wireless network, you can enable more security and fine-tune the access point by modifying its advanced configuration features.

Make Sure the Access Point is Connected to the LAN

If you configured the access point and administrator PC by connecting both into a network hub, then your access point is already connected to the LAN.

If you configured the access point using a direct wired connection via Ethernet cable from your computer to the access point, do the following:

1. Disconnect the Ethernet cable from the computer.
2. Connect the free end of the cable to the LAN.
3. Connect your computer to the LAN either via Ethernet cable or wireless client card.

Test LAN Connectivity with Wireless Clients

Test the Professional Access Point by trying to detect it and associate with it from a wireless client device. (See “Wireless Client Computers” on page 19 in the Pre-Launch Checklist: Default Settings and Supported Administrator/Client Platforms for information on requirements for these clients.)

Secure and Fine-Tune the Access Point Using Advanced Features

Once the wireless network is operational and has been tested with a wireless client, you can add more security, add users, configure a Guest interface, and fine-tune the access point performance settings.

Web User Interface

This part of the Professional Access Point Administrator Guide covers usage of the Web User Interface with each section corresponding to a menu section:

- “Basic Settings” on page 35
- “Cluster” on page 43
- “Status” on page 77
- “Advanced” on page 89

Basic Settings

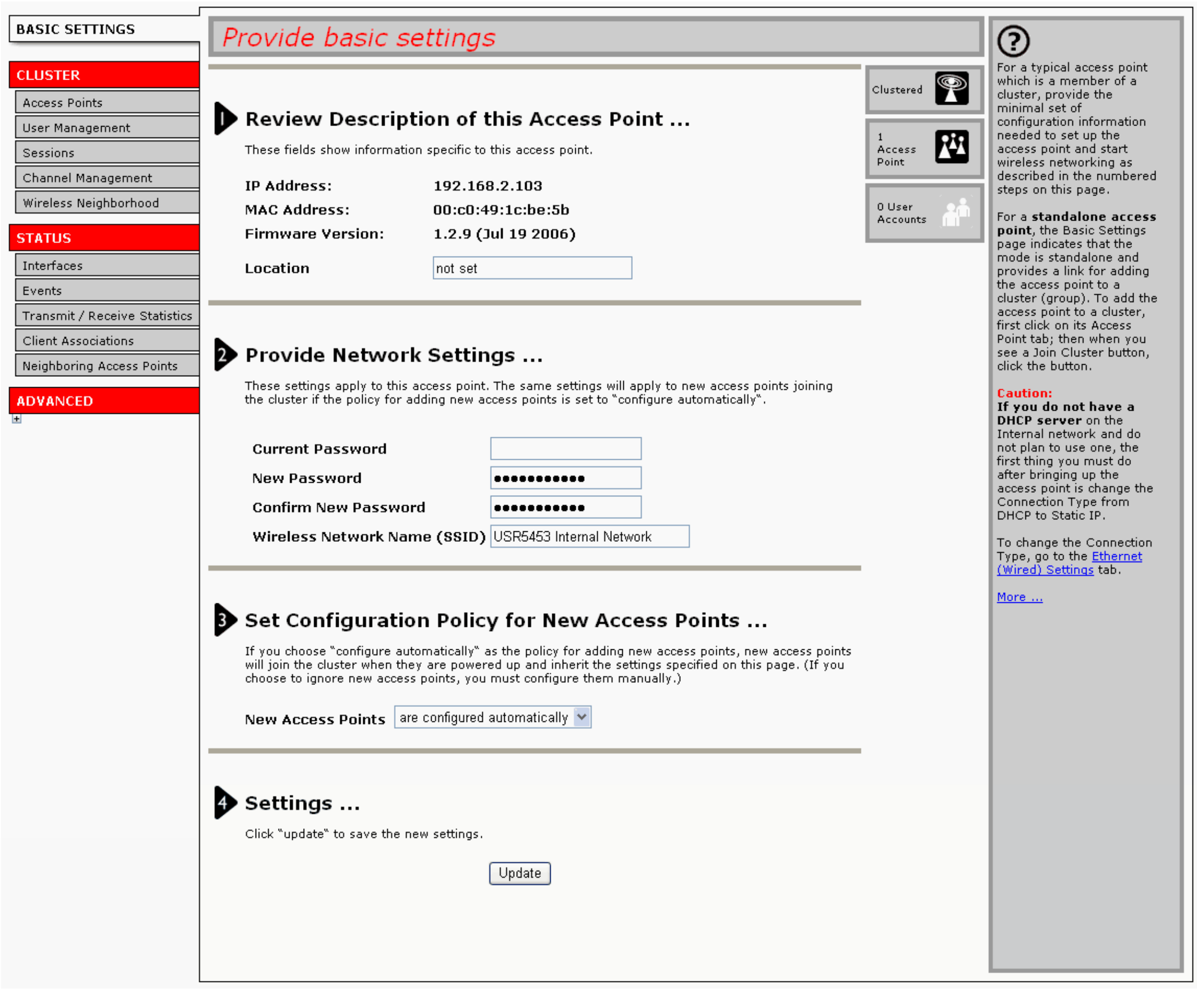
The basic configuration tasks are described in the following sections:

- Navigating to Basic Settings
- Review / Describe the Access Point
- Provide Administrator Password and Wireless Network Name
- Set Configuration Policy for New Access Points
- Update Basic Settings
- Summary of Settings
- Basic Settings for a Standalone Access Point
- Your Network at a Glance: Understanding Indicator Icons

Navigating to Basic Settings

To configure initial settings, click **Basic Settings**.

If you use the Detection Utility to link to the Web User Interface, the Basic Settings page is displayed by default.



Provide basic settings

1 Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 192.168.2.103
MAC Address: 00:c0:49:1c:be:5b
Firmware Version: 1.2.9 (Jul 19 2006)
Location: not set

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

Current Password
New Password: ●●●●●●●●●●●●
Confirm New Password: ●●●●●●●●●●●●
Wireless Network Name (SSID): USR5453 Internal Network

3 Set Configuration Policy for New Access Points ...

If you choose "configure automatically" as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points: are configured automatically

4 Settings ...

Click "update" to save the new settings.

For a typical access point which is a member of a cluster, provide the minimal set of configuration information needed to set up the access point and start wireless networking as described in the numbered steps on this page.

For a **standalone access point**, the Basic Settings page indicates that the mode is standalone and provides a link for adding the access point to a cluster (group). To add the access point to a cluster, first click on its Access Point tab; then when you see a Join Cluster button, click the button.

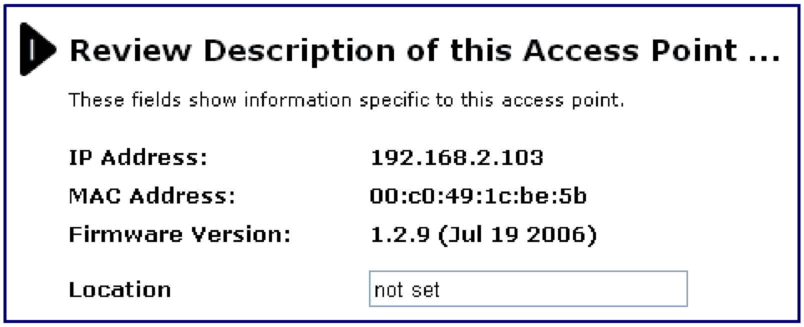
Caution:
If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

To change the Connection Type, go to the Ethernet (Wired) Settings tab.

More ...

Fill in the fields on the Basic Settings page as described below.

Review / Describe the Access Point



Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 192.168.2.103

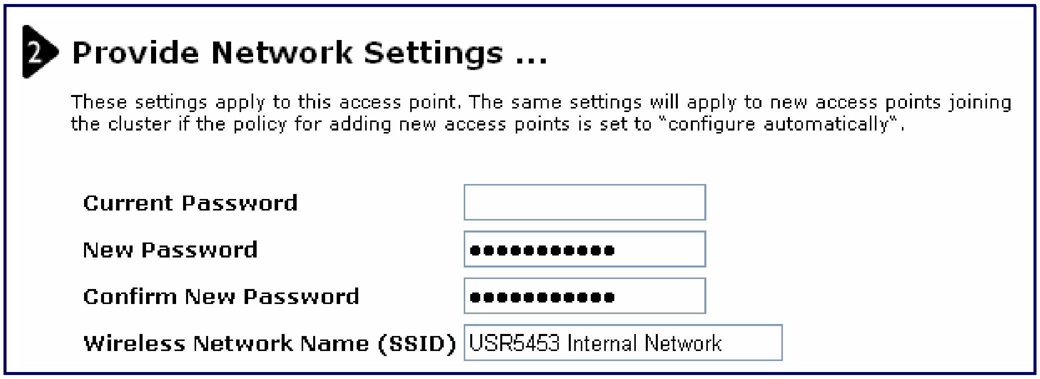
MAC Address: 00:c0:49:1c:be:5b

Firmware Version: 1.2.9 (Jul 19 2006)

Location: not set

Field	Description
IP Address	The IP address assigned to this access point. This field is not editable because the IP address is already assigned (either via DHCP, or statically through the Ethernet (wired) settings as described in “Configuring Guest Interface Ethernet (Wired) Settings” on page 95).
MAC Address	The MAC address of the access point. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is displayed for informational purposes as a unique identifier for an interface. The address shown here is the MAC address for the bridge (`br0`). This is the address by which the access point is known externally to other networks. To see MAC addresses for Guest and Internal interfaces on the access point, go to the Status menu and view the Interface tab.
Firmware Version	Version information about the firmware currently installed on the access point. As new versions of the Professional Access Point firmware become available, you can upgrade the firmware on your access points to take advantages of new features and enhancements. For instructions on how to upgrade the firmware, see “Upgrade” on page 172.
Location	Specify a location description for this access point.

Provide Administrator Password and Wireless Network Name



Provide Network Settings ...

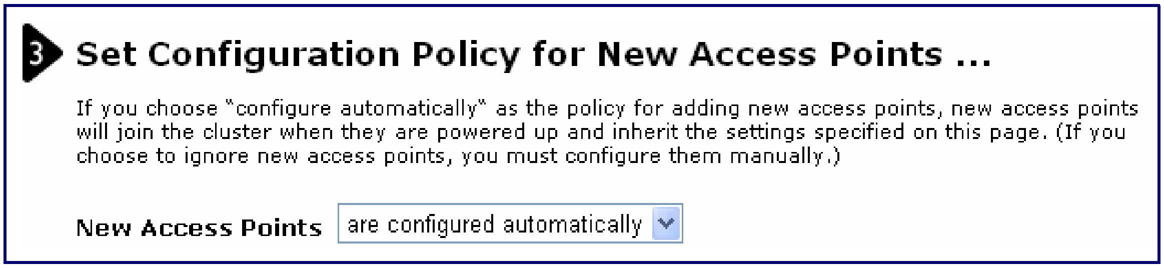
These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

Current Password	
New Password	●●●●●●●●●●●●
Confirm New Password	●●●●●●●●●●●●
Wireless Network Name (SSID)	USR5453 Internal Network

Field	Description
Administrator Password	Enter a new administrator password. The characters you enter will be displayed as "•" characters to prevent others from seeing your password as you type. The Administrator password must be an alphanumeric string of up to 8 characters. Do not use special characters or spaces. ▶ As an immediate first step in securing your wireless network, USRobotics recommends that you change the administrator password from the default.
Administrator Password (again)	Re-enter the new password to confirm that you typed it as you intended.
Wireless Network Name (SSID)	Enter a name for the wireless network. This name will apply to all access points on this network. As you add more access points, they will share this SSID. The *Service Set Identifier* (SSID) must be an alphanumeric string of up to 32 characters **Note:** If you are connected as a wireless client to the access point that you are administering, resetting the SSID will cause you to lose connectivity to the access point. You will need to reconnect using the new SSID.

Note The Professional Access Point is not designed for multiple, simultaneous configuration changes. If more than one administrator is making changes to the configuration at the same time, all access points in the cluster will stay synchronized, but there is no guarantee that all changes specified by all of the administrators will be applied.

Set Configuration Policy for New Access Points



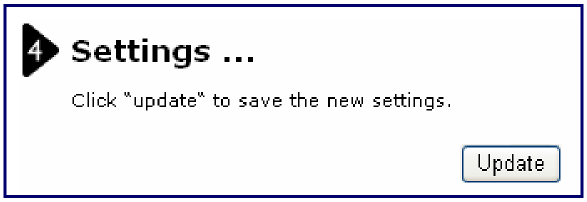
Set Configuration Policy for New Access Points ...

If you choose "configure automatically" as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points: are configured automatically

Field	Description
New Access Points	Choose the policy that you want to put in effect for adding New Access Points to the network. • If you choose **are configured automatically**, then when a new access point is added to the network it automatically joins the existing *cluster*. The cluster configuration is copied to the new access point, and no manual configuration is required to deploy it. • If you choose **are ignored**, new access points will not join the cluster; they will be considered *standalone*. You need to configure standalone access points manually via the Detection Utility and the Web User Interface residing on the standalone access points. (To get to the Web page for a standalone access point, use its IP address in a URL as follows: http://*IPAddressOfAccessPoint*.) **Note:** If you change the policy so that new access points are ignored, then any new access points you add to the network will not join the cluster. Existing clustered access points will not be aware of these standalone APs. Therefore, if you are viewing the Web User Interface via the IP address of a clustered access point, the new standalone APs will not show up in the list of access points on the Cluster menu's Access Points page. The only way to see a standalone access point is to browse to it directly by using its IP address as the URL. If you later change the policy back to the default so that new access points are configured automatically, all subsequent new APs will automatically join the cluster. Standalone APs, however, will stay in standalone mode until you explicitly add them to the cluster. For information on how to add standalone APs to the cluster, see "Adding an Access Point to a Cluster" on page 50.

Update Basic Settings



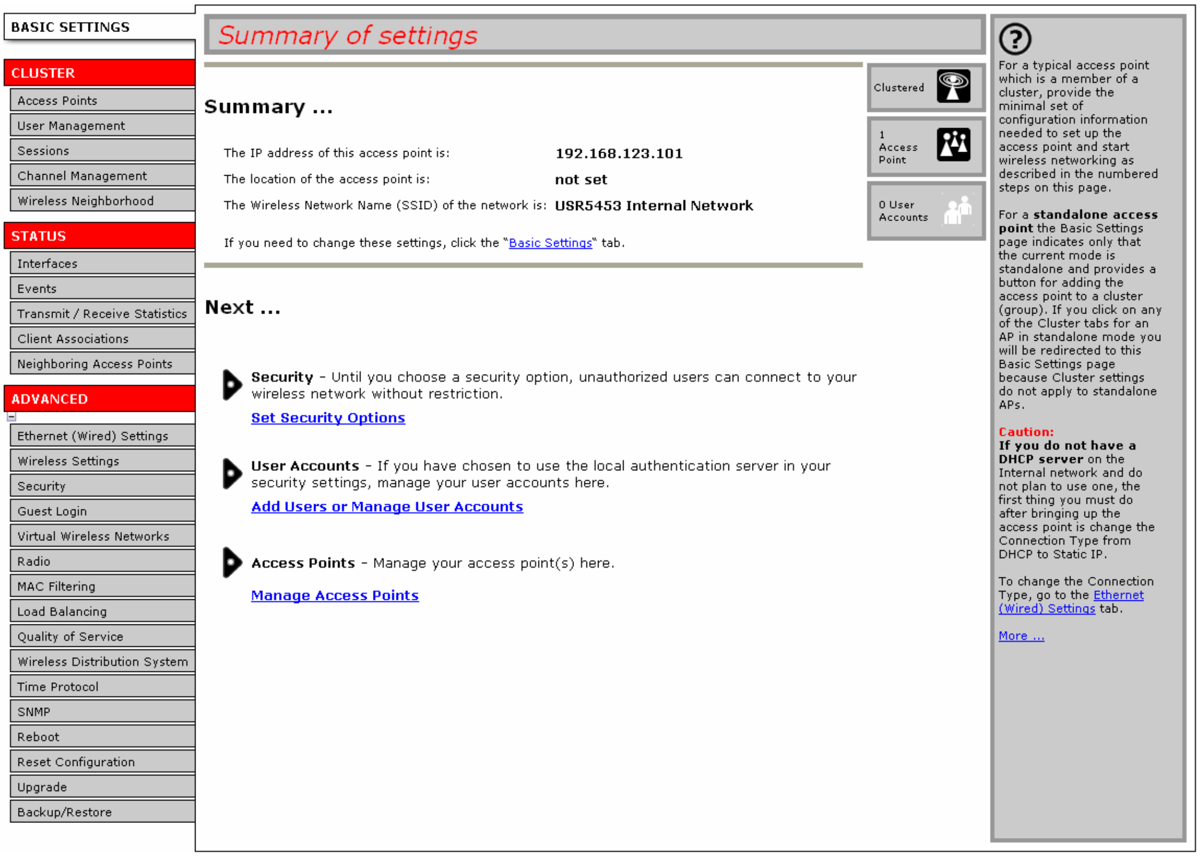
Settings ...

Click "update" to save the new settings.

When you have reviewed the new configuration, click **Update** to apply the settings and deploy the access points as a wireless network.

Summary of Settings

When you update the **Basic Settings**, a summary of the new settings is shown along with information about next steps.



Summary of settings

Summary ...

The IP address of this access point is: **192.168.123.101**

The location of the access point is: **not set**

The Wireless Network Name (SSID) of the network is: **USR5453 Internal Network**

If you need to change these settings, click the "Basic Settings" tab.

Next ...

Security - Until you choose a security option, unauthorized users can connect to your wireless network without restriction.

Set Security Options

User Accounts - If you have chosen to use the local authentication server in your security settings, manage your user accounts here.

Add Users or Manage User Accounts

Access Points - Manage your access point(s) here.

Manage Access Points

For a typical access point which is a member of a cluster, provide the minimal set of configuration information needed to set up the access point and start wireless networking as described in the numbered steps on this page.

For a **standalone access point** the Basic Settings page indicates only that the current mode is standalone and provides a button for adding the access point to a cluster (group). If you click on any of the Cluster tabs for an AP in standalone mode you will be redirected to this Basic Settings page because Cluster settings do not apply to standalone APs.

Caution:
If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

To change the Connection Type, go to the Ethernet (Wired) Settings tab.

More ...

At initial startup, no security is in place on the access point. An important next step is to configure security, as described in “Security” on page 101.

At this point if you click Basic Settings again, the summary of settings page is replaced by the standard Basic Settings configuration options.

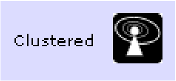
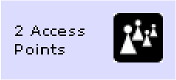
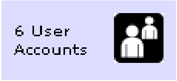
Basic Settings for a Standalone Access Point

The Basic Settings page for a standalone access point indicates that the mode is standalone and provides a link for adding the access point to a cluster (group). If you click on any of the Cluster tabs on the Web User Interface pages for an access point in standalone mode, you will be redirected to the Basic Settings page because Cluster settings do not apply to standalone APs.

For more information see “Standalone Mode” on page 47 and “Adding an Access Point to a Cluster” on page 50.

Your Network at a Glance: Understanding Indicator Icons

All the Cluster settings tabs on the Web User Interface include icons that show current network activity.

Icon	Description
 Clustered	When one or more APs on your network are available for service, the Wireless Network Available icon is shown. The clustering icon indicates whether the current access point is **Clustered** or **Not Clustered** (that is, standalone). For information about clustering, see “Understanding Clustering” on page 44.
 2 Access Points	The number of access points available for service on this network is indicated by the Access Points icon. For information about managing access points, see “Access Points” on page 43.
 6 User Accounts	The number of user accounts created and enabled on this network is indicated by the User Accounts icon. For information about setting up user accounts on the access point for use with the built-in authentication server, see “User Management” on page 53. See also “IEEE 802.1x” on page 114 and “WPA/WPA2 Enterprise (RADIUS)” on page 117, which are the two security modes that offer the option of using the built-in authentication server.

Cluster

This section covers the Web User Interface Cluster items:

Access Points

The Professional Access Point shows current basic configuration settings for clustered access points (location, IP address, MAC address, status, and availability) and provides a way of navigating to the full configuration for specific APs if they are cluster members.

Standalone access points or those which are not members of this cluster do not show up in this listing. To configure standalone access points, you must discover (via the Detection Utility) or know the IP address of the access point and by using its IP address in a URL (`http://`*`IPAddressOfAccessPoint`*).

Note The Professional Access Point is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the Web User Interface and making changes to the configuration, all access points in the cluster will stay synchronized but there is no guarantee that all configuration changes specified by multiple users will be applied.

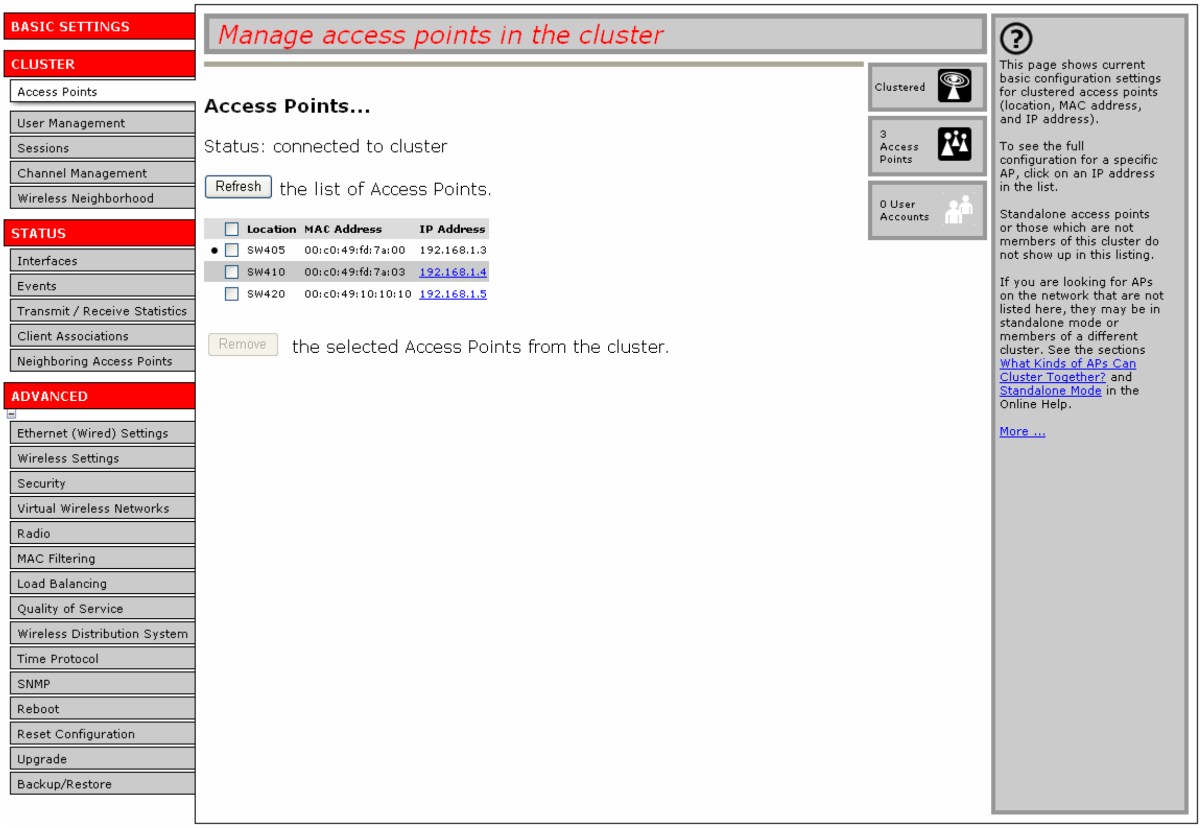
The following topics are covered:

- Navigating to Access Points Management
- Understanding Clustering
    - What is a Cluster?
    - How Many APs Can a Cluster Support?
    - What Kinds of APs Can Cluster?
    - Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?
    - Cluster Mode
    - Standalone Mode
    - Cluster Formation

  - Cluster Size and Membership
  - Intra-Cluster Security
  - Auto-Synchronization of Cluster Configuration
- Understanding Access Point Settings
- Modifying the Location Description
- Removing an Access Point from the Cluster
- Adding an Access Point to a Cluster
- Navigating to the Web User Interface for a Specific Access Point

Navigating to Access Points Management

To view or edit information on access points in a cluster, click the Cluster menu's **Access Points** tab.



Manage access points in the cluster

Access Points...

Status: connected to cluster

[Refresh] the list of Access Points.

	□	Location	MAC Address	IP Address
●	□	SW405	00:c0:49:fd:7a:00	192.168.1.3
	□	SW410	00:c0:49:fd:7a:03	192.168.1.4
	□	SW420	00:c0:49:10:10:10	192.168.1.5

[Remove] the selected Access Points from the cluster.

This page shows current basic configuration settings for clustered access points (location, MAC address, and IP address).

To see the full configuration for a specific AP, click on an IP address in the list.

Standalone access points or those which are not members of this cluster do not show up in this listing.

If you are looking for APs on the network that are not listed here, they may be in standalone mode or members of a different cluster. See the sections What Kinds of APs Can Cluster Together? and Standalone Mode in the Online Help.

More ...

Understanding Clustering

A key feature of the Professional Access Point is the ability to form a dynamic, configuration-aware group (called a *cluster*) with other Professional Access Points in a network in the same subnet. Access points can participate in a self-organizing cluster which makes it easier for you to deploy, administer, and secure your wireless network. The cluster provides a single point of administration and lets you view the deployment of access points as a single wireless network rather than a series of separate wireless devices.

What is a Cluster?

A cluster is a group of access points which are coordinated as a single group via Professional Access Point administration. You cannot create multiple clusters on a single wireless network (SSID). Only one cluster per wireless network is supported.

How Many APs Can a Cluster Support?

Up to eight access points are supported in a cluster at any one time. If a new access point is added to a network with a cluster that is already at full capacity, the new access point is added in *standalone mode*. Note that when the cluster is full, extra APs are added in stand-alone mode regardless of the configuration policy in effect for new access points.

For related information, see “Cluster Mode” on page 47, “Standalone Mode” on page 47, and “Set Configuration Policy for New Access Points” on page 39.

What Kinds of APs Can Cluster?

A single Professional Access Point can form a cluster with itself (a cluster of one) and with other Professional Access Points of the same model. In order to be members of the same cluster, access points must be on the same LAN.

Having a mix of APs on the network does not adversely affect Professional Access Point clustering in any way. However, access points of other types will not join the cluster. Those APs must be administered with their own associated administration tools.

Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?

Most configuration settings defined via the Professional Access Point Web User Interface will be propagated to cluster members as a part of the *cluster configuration*.

Settings Shared in the Cluster Configuration

The cluster configuration includes:

- Network name (SSID)
- Administrator Password
- Configuration policy
- User accounts and authentication
- Wireless interface settings
- Guest Welcome screen settings
- Network Time Protocol (NTP) settings

- Radio settings

  The following radio settings are synchronized across clusters:

  - Mode
  - Channel

    Note When **Channel Planning** is enabled, the radio Channel is not synchronized across the cluster. See “Stopping/Starting Automatic Channel Assignment” on page 66.

  - Fragmentation Threshold
  - RTS Threshold
  - Rate Sets

  The following radio settings are *not* synchronized across clusters:

  - Beacon Interval
  - DTIM Period
  - Maximum Stations
  - Transmit Power

- Security settings
- QoS queue parameters
- MAC address filtering

Settings Not Shared by the Cluster

The few exceptions (settings *not* shared among clustered access points) are the following; most of these, by their nature, must be unique:

- IP addresses
- MAC addresses
- Location descriptions
- Load Balancing settings
- WDS bridges
- Ethernet (Wired) Settings, including enabling or disabling Guest VLAN access
- Guest VLAN interface configuration

Settings that are not shared must be configured individually in the Web User Interface for each access point. To access the Web User Interface for an access point that is a member of the current cluster, click the Cluster menu's **Access Points** tab in the Web User Interface of the current access point, then click the member access point's **IP Address** link.

Cluster Mode

When an access point is a cluster member, it is considered to be in cluster mode. You define whether you want new access points to join the cluster or not via the configuration policy you set in the Basic Settings. (See "Set Configuration Policy for New Access Points" on page 39.) You can reset an access point in cluster mode to standalone mode. (See "Removing an Access Point from the Cluster" on page 49.)

Note When the cluster is full (eight APs is the limit), extra APs are added in *stand-alone mode* regardless of the configuration policy in effect for new access points.

Standalone Mode

The Professional Access Point can be configured in *standalone* mode. In standalone mode, an access point is not a member of the cluster and does not share the cluster configuration, but rather requires manual configuration that is not shared with other access points. (See "Set Configuration Policy for New Access Points" on page 39 and "Removing an Access Point from the Cluster" on page 49.)

Standalone access points are not listed on the Cluster menu's Access Points page in the Web User Interfaces of APs that are cluster members. You need to know the IP address for a standalone access point in order to configure and manage it directly. (See "Navigating to an Access Point by Using its IP Address in a URL" on page 50.)

The Basic Settings tab for a standalone access point indicates that the mode is standalone and provides a link for adding the access point to a cluster (group). If you click any of the Cluster tabs in the Web User Interface for a standalone access point, you will be redirected to the Basic Settings page because Cluster settings do not apply to standalone APs.

Note When the cluster is full, new APs are added in *standalone mode* regardless of the configuration policy in effect for new access points. A cluster supports a maximum of eight access points.

You can re-enable cluster mode on a standalone access point. (See "Adding an Access Point to a Cluster" on page 50.)

Cluster Formation

A cluster is formed when the first Professional Access Point is configured. (See "Setting Up and Launching Your Wireless Network" on page 23 and "Basic Settings" on page 35.)

If a cluster configuration policy in place, when a new access point is deployed, it attempts to rendezvous with an existing cluster.

If it is unable to locate a cluster, then it establishes a new cluster on its own.

If it locates a cluster but is rejected because the cluster is full or because the clustering policy is to ignore new access points, then the access point deploys in standalone mode.

Cluster Size and Membership

The upper limit of a cluster is eight access points. The Cluster Web User Interface pages provide a visual indicator of the number of access points in the current cluster and warn when the cluster has reached capacity.

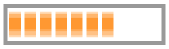
Intra-Cluster Security

To ensure that the security of the cluster as a whole is equivalent to the security of a single access point, communication of certain data between access points in a cluster is accomplished through Secure Sockets Layer (typically referred to as *SSL*) with private key encryption.

Both the cluster configuration file and the user database are transmitted among access points using SSL.

Auto-Synchronization of Cluster Configuration

If you are making changes to the access point configuration that require a relatively large amount of processing (such as adding several new users), you may encounter a synchronization progress bar after clicking Update on any of the Web User Interface pages. The progress bar indicates that the system is busy performing an auto-synchronization of the updated configuration across all APs in the cluster. The Web User Interface pages are not editable during the auto-synch.



Note that auto-synchronization always occurs during configuration updates that affect the cluster, but the processing time is usually negligible. The auto-synchronization progress bar is displayed only for longer-than-usual wait times.

Understanding Access Point Settings

The Access Points tab provides information about all access points in the cluster.

From this tab, you can view location descriptions, IP addresses, enable (activate) or disable (deactivate) *clustered* access points, and remove access points from the cluster. You can also modify the location description for an access point.

The IP address links provide a way to navigate to configuration settings and data on an access point.

Standalone access points (those which are not members of the cluster) are not shown on this page.

The following table describes the access point settings and information display in detail.

Field	Description
Location	Description of the access point's physical location.
MAC Address	Media Access Control (MAC) address of the access point. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point. The address shown here is the MAC address for the bridge (`br0`). This is the address by which the access point is known externally to other networks. To see MAC addresses for Guest and Internal interfaces on the access point, see the Status menu's Interfaces page.
IP Address	Specifies the IP address for the access point. Each IP address is a link to the Web User Interface for that access point. You can use the links to navigate to the Web User Interface for a specific access point. This is useful for viewing data on a specific access point to make sure a cluster member is picking up cluster configuration changes, to configure advanced settings on a particular access point, or to switch a standalone access point to cluster mode.

Modifying the Location Description

To make modifications to the location description:

1. Navigate to the **Basic Settings** page.
2. Update the **Location** description in section 1 under **Review Description of this Access Point**.
3. Click **Update** button to apply the changes.

Removing an Access Point from the Cluster

To remove an access point from the cluster, do the following.

1. Select the check box next to the access point.
2. Click **Remove** from Cluster.

   The change will be reflected under Status for that access point; the access point will now show as *standalone* (instead of *cluster*).

Note In some situations, it is possible for the cluster to lose synchronization. If, after removing an access point from the cluster, the access point list still reflects the deleted access point or shows an incomplete display, refer to the information on Cluster Recovery in “Troubleshooting”.

Adding an Access Point to a Cluster

To add a standalone access point into a cluster, do the following.

1. Go to the Web User Interface for the standalone access point. (See “Navigating to an Access Point by Using its IP Address in a URL” on page 50.)

   The Web User Interface pages for the standalone access point are displayed.

2. Click the **Basic Settings** tab in the **Administration** pages for the standalone access point.

   The Basic Settings tab for a standalone access point indicates that the mode is standalone and provides a link for adding the access point to a cluster (group).

   Note If you click any of the Cluster tabs in the Web User Interface for an access point in standalone mode, you will be redirected to the Basic Settings page because Cluster settings do not apply to standalone APs.

3. Click the **Access Point** tab.

   A Join Cluster button appears.

4. Click the **Join Cluster** button.

   The access point is now a cluster member. Its Status (Mode) on the Cluster menu’s Access Points page now indicates **cluster** instead of **standalone**.

Navigating to the Web User Interface for a Specific Access Point

In general, the Professional Access Point is designed for central management of *clustered* access points. All access points in a cluster reflect the same configuration. In this case, it does not matter which access point you actually connect to for administration.

There may be situations, however, when you want to view or manage information on a particular access point. For example, you might want to check status information such as client associations or events for an access point. You can navigate to the Web User Interface for an individual access point by clicking the access point’s IP address link on the Access Points tab.

All clustered access points are shown on the Cluster menu’s Access Points page. To navigate to clustered access points, you can simply click on the IP address for a specific cluster member shown in the list.

Navigating to an Access Point by Using its IP Address in a URL

You can also link to the Web User Interface of a specific access point by entering the IP address for that access point as a URL directly into a Web browser address bar in the following form:

```
http://IPAddressOfAccessPoint
```

where *IPAddressOfAccessPoint* is the address of the particular access point that you want to monitor or configure.

For a standalone access point, this is the only way to navigate to the configuration information.

If you do not know the IP address for a standalone access point, use the Detection Utility to find all APs on the network and you should be able to derive which ones are standalone by comparing the Detection Utility findings with access points listed on the Cluster menu's Access Points page. The APs that the Detection Utility finds that are not shown on the Access Points page are probably standalone APs. (For more information on using the Detection Utility, see "Step 3. Run the Detection Utility to find access points on the network" on page 26.)

User Management

The Professional Access Point includes user management capabilities for controlling access to your access points.

User management and authentication must always be used in conjunction with the following two security modes, which require use of a RADIUS server for user authentication and management.

- IEEE 802.1x mode (see “IEEE 802.1x” on page 114 in Security)
- WPA with RADIUS mode (see “WPA/WPA2 Enterprise (RADIUS)” on page 117 in Security)

You have the option of using either the internal RADIUS server embedded in the Professional Access Point or an external RADIUS server that you provide. If you use the embedded RADIUS server, use this Administration Web page on the access point to set up and manage user accounts. If you are using an external RADIUS server, you will need to set up and manage user accounts for that server in the Web User Interface.

On the User Management page, you can create, edit, remove, and view *user accounts*. Each user account consists of a user name and password. The set of users specified on the User Management page represent approved *clients* that can log in and use one or more access points to access local and possibly external networks via your wireless network.

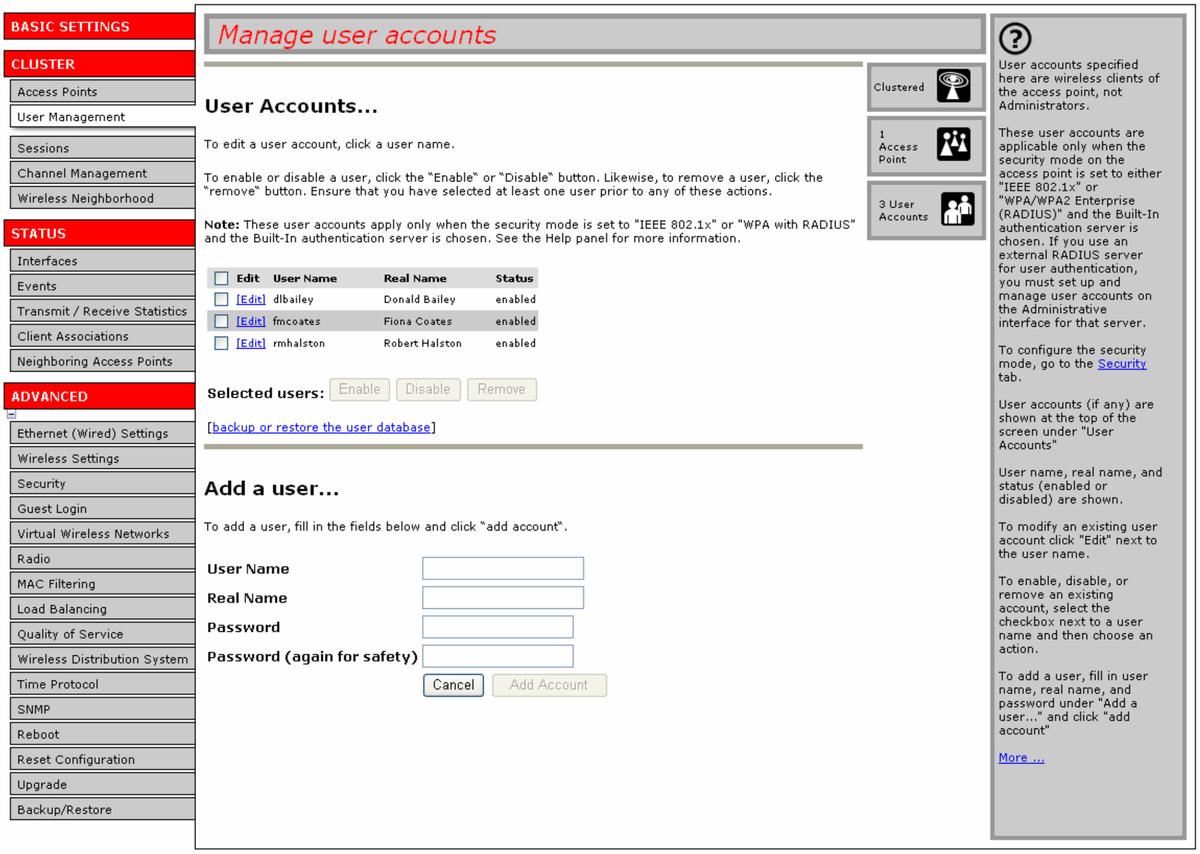
Note Users specified on the User Management page are those who use the APs as a connectivity hub, not administrators of the wireless network. Only those with the administrator user name and password and knowledge of the administration URL can log in as an administrator and view or modify configuration settings.

The following topics are covered:

- Navigating to User Management for Clustered Access Points
- Viewing User Accounts
- Adding a User
- Editing a User Account
- Enabling and Disabling User Accounts
- Removing a User Account
- Backing Up and Restoring a User Database

Navigating to User Management for Clustered Access Points

To set up or modify user accounts, click the Cluster Menu's **User Management** tab.



Manage user accounts

User Accounts...

To edit a user account, click a user name.

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "remove" button. Ensure that you have selected at least one user prior to any of these actions.

Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

□	Edit	User Name	Real Name	Status
□	[Edit]	dlbailey	Donald Bailey	enabled
□	[Edit]	fmcoates	Fiona Coates	enabled
□	[Edit]	rmhalston	Robert Halston	enabled

Selected users: Enable Disable Remove

[backup or restore the user database]

Add a user...

To add a user, fill in the fields below and click "add account".

User Name	
Real Name	
Password	
Password (again for safety)	

Cancel Add Account

User accounts specified here are wireless clients of the access point, not Administrators.

These user accounts are applicable only when the security mode on the access point is set to either "IEEE 802.1x" or "WPA/WPA2 Enterprise (RADIUS)" and the Built-In authentication server is chosen. If you use an external RADIUS server for user authentication, you must set up and manage user accounts on the Administrative interface for that server.

To configure the security mode, go to the Security tab.

User accounts (if any) are shown at the top of the screen under "User Accounts"

User name, real name, and status (enabled or disabled) are shown.

To modify an existing user account click "Edit" next to the user name.

To enable, disable, or remove an existing account, select the checkbox next to a user name and then choose an action.

To add a user, fill in user name, real name, and password under "Add a user..." and click "add account"

More ...

Viewing User Accounts

User accounts are shown at the top of the screen under **User Accounts**. User name, real name, and status (enabled or disabled) are shown.

Adding a User

To create a new user, do the following:

1. Under **Add a User**, provide information in the following fields.

Field	Description
Username	Provide a user name. The user name is an alphanumeric string of up to 237 characters. Do not use special characters or spaces.

Field	Description
Real Name	For information purposes, provide the user's full name. Real name is a maximum of 256 characters long.
Password	Specify a password for this user. The password is an alphanumeric string of up to 256 characters. Do not use special characters or spaces.

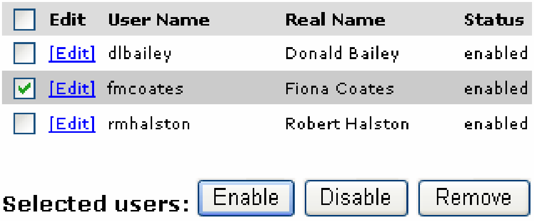
2. When you have filled in the fields, click **Add Account** to add the account.

   The new user is then displayed under **User Accounts.** The user account is **enabled** by default when you first create it.

Note A limit of 100 user accounts per access point is imposed by the Web User Interface. Network usage may impose a more practical limit, depending upon the demand from each user.

Editing a User Account

Once you have created a user account, it is displayed under **User Accounts** at the top of the User Management Administration Web page. To modify an existing user account, first select **[Edit]** next to the user name.



□	Edit	User Name	Real Name	Status
□	[Edit]	dlbailey	Donald Bailey	enabled
☑	[Edit]	fmcoates	Fiona Coates	enabled
□	[Edit]	rmhalston	Robert Halston	enabled

Then, make your changes in the Update Account section of the page and click **Update Account**.

Enabling and Disabling User Accounts

A user account must be enabled for the user to log on and use the access point.

You can enable or disable any user account. With this feature, you can maintain a set of user accounts and authorize or prevent users from accessing the network without having to remove or re-create accounts. This ability is useful in situations where users have an occasional need to access the network. For example, contractors who do work for your company on an intermittent but regular basis might need network access for 3 months at a time, then be off for 3 months, and back on for another assignment. You can enable and disable these user accounts as needed, and control access as appropriate.

Enabling a User Account

To enable a user account, select the check box next to the user name and click **Enable**.

A user with an account that is enabled can log on to the wireless access points in your network.

Disabling a User Account

To disable a user account, select the check box next to the user name and click **Disable**.

A user with an account that is disabled cannot log on to the wireless access points in your network. However, the user account remains in the database and can be enabled later as needed.

Removing a User Account

To remove a user account, select the check box next to the user name and click **Remove**.

If you think that you might need to add this user again at a later date, you might consider disabling the user account rather than removing it.

Backing Up and Restoring a User Database

You can save a copy of the current set of user accounts to a backup configuration file. The backup file can be used at a later date to restore the user accounts on the access point to the previous configuration.

Backing Up the User Database

To create a backup copy of the user accounts for the access point:

1. Click the **backup or restore the user database** link; then click **backup user database**.

   A File Download or Open dialogue box is displayed.

2. Choose the **Save** option.

   A file browser is displayed.

3. Use the file browser to navigate to the directory where you want to save the file, and click **OK** to save the file.

   You can use the default file name (`wirelessUsers.ubk`) or specify a new file name, but be sure to save the file with a `.ubk` extension.

Restoring a User Database from a Backup File

To restore a user database from a backup file:

1. Click the **backup or restore the user database** link; then click **restore user database**.

2. Select the backup configuration file that you want to use, either by typing the full path and file name in the **Restore** field or by clicking **Browse** and selecting the file.

   (Only those files that were created with the **User Database Backup** function and saved as `.ubk` backup configuration files are valid to use with **Restore**; for example, `wirelessUsers.ubk`.)

3. Click the **Restore** button.

   When the backup restore process is complete, a message indicates that the user database has been successfully restored. (This process is not time-consuming; the restore should complete almost immediately.)

   Click the Cluster menu’s **User Management** tab to see the restored user accounts.

Sessions

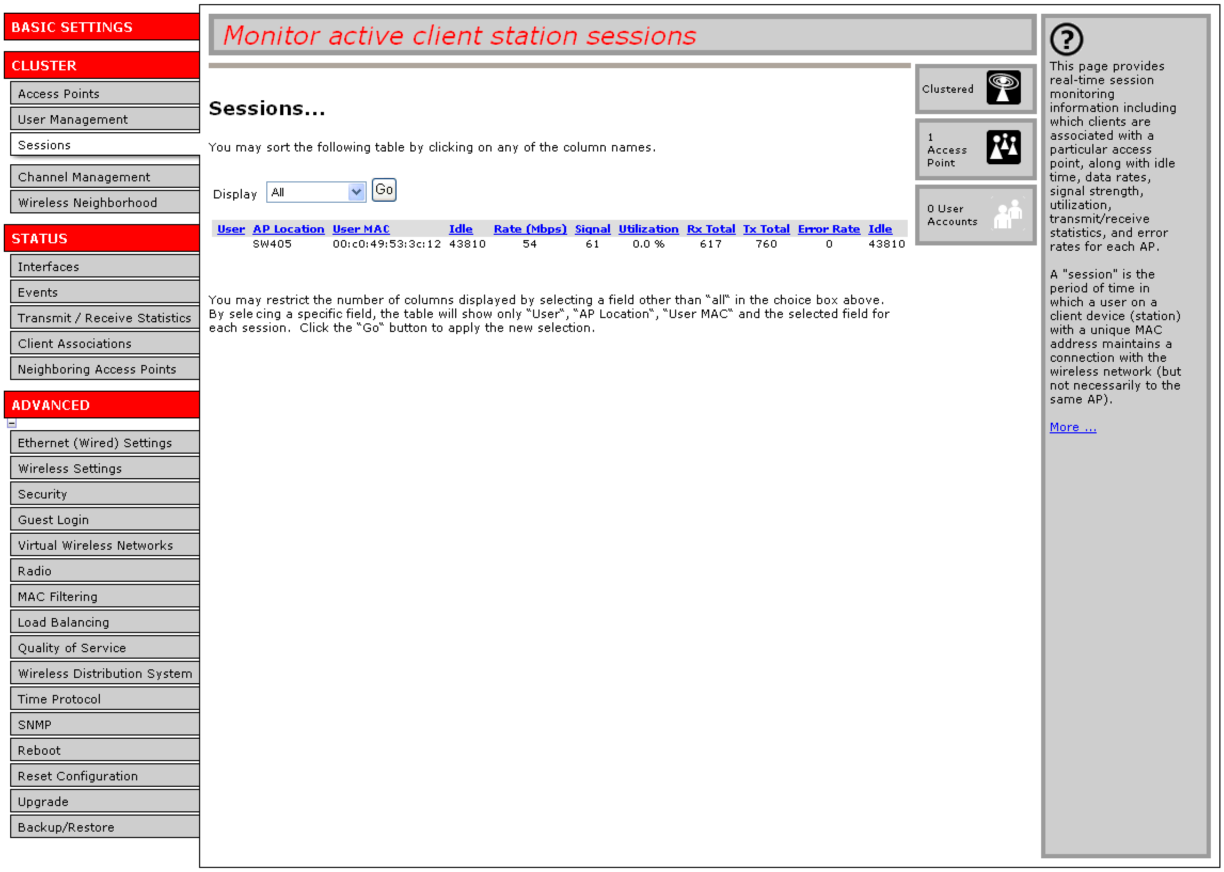
The Professional Access Point provides real-time session monitoring information including which users and clients are associated with a particular access point, data rates, transmit/receive statistics, signal strength, and idle time.

The following Session Monitoring topics are covered here:

- Navigating to Session Monitoring
- Understanding Session Monitoring Information
- Viewing Session Information for Access Points
- Sorting Session Information
- Refreshing Session Information

Navigating to Session Monitoring

To view session monitoring information, click the Cluster menu’s **Sessions** tab.



Sessions...

You may sort the following table by clicking on any of the column names.

User	AP Location	User MAC	Idle	Rate (Mbps)	Signal	Utilization	Rx Total	Tx Total	Error Rate	Idle
	SW405	00:c0:49:53:3c:12	43810	54	61	0.0 %	617	760	0	43810

You may restrict the number of columns displayed by selecting a field other than “all” in the choice box above. By sele cing a specific field, the table will show only “User”, “AP Location”, “User MAC” and the selected field for each session. Click the “Go” button to apply the new selection.

This page provides real-time session monitoring information including which clients are associated with a particular access point, along with idle time, data rates, signal strength, utilization, transmit/receive statistics, and error rates for each AP.

A "session" is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network (but not necessarily to the same AP).

Understanding Session Monitoring Information

The Sessions page shows information about users and client devices associated with access points in the cluster. Each session is identified by user name and client MAC address, along with the access point (location) to which the client is connected.

To view a particular statistic for a session, select the item from the **Display** list and click **Go**. You can view Idle Time, Data Rate, Signal, Utilization, and so on; all of which are described in detail in the table below.

A *session* is the period of time for which a user on a client device with a unique MAC address maintains a connection with the wireless network. The session begins when the user logs on to the *network*, and the session ends when the user either logs off intentionally or loses the connection unintentionally.

Note

A *session* is not the same as an *association*, which describes a client connection to a particular access point. A client network connection can shift from one clustered access point to another within the context of the same session. A client station can roam between APs and maintain the session.

For information about monitoring *associations* and *link integrity monitoring*, see “Client Associations” on page 83.

Details about session information are given below.

Field	Description
User	The user names of IEEE 802.1x clients. **Note:** This field is relevant only for clients that are connected to APs using IEEE 802.1x security mode *and* local authentication server. (For more information about this mode, see “IEEE 802.1x” on page 114.) For clients of APs using IEEE 802.1x with RADIUS server or other security modes, no user name will be shown here.
AP Location	The location of the access point. This is derived from the location description specified on the Basic Settings tab.
User MAC	The MAC address of the user’s client device. A MAC address is a hardware address that uniquely identifies each node of a network.
Idle	The amount of time that this station has remained inactive. A station is considered to be idle when it is not receiving or transmitting data. Idle time is measured in milliseconds.
Rate	The speed at which this access point is transferring data to the client. The data transmission rate is measured in megabits per second (Mbps). This value will fall within the range of the advertised rate set for the IEEE 802.1x mode in use on the access point. For example, 1 to 54Mbps for 802.11g.

Field	Description
Signal	Indicates the strength of the radio frequency (RF) signal the client receives from the access point. The measure used for this is an IEEE 802.1x value known as *Received Signal Strength Indication* (RSSI), and is a value between 0 and 100. RSSI is determined by a an IEEE 802.1x mechanism implemented on the network interface card (NIC) of the client.
Utilization	Utilization rate for this station. For example, if the station is active (transmitting and receiving data) 90% of the time and inactive 10% of the time, its utilization rate is 90%.
Rx Total	Receive Total: Indicates number of total packets received by the client during the current session.
Tx Total	Transmit Total: Indicates number of total packets transmitted to the client during this session.
Error Rate	Indicates the percentage frames that are dropped during transmission on this access point.

Viewing Session Information for Access Points

You can view session information for all access points on the network at the same time, or you can set the display to show session information for a specified access point chosen from the list at the top of the page.

To view information on all access points, select **Show all access points** at the top of the page.

To view session information on a particular access point, select **Show only this access point** and select the access point name from the list.

Sorting Session Information

To order (sort) the information in the tables, click on the column label by which you want to order the information rows. For example, if you want to see the table rows ordered by utilization rate, click on the **Utilization** column label. The entries will be sorted by utilization rate.

Refreshing Session Information

You can force an update of the information displayed on the Session Monitoring page by clicking the **Refresh** button.

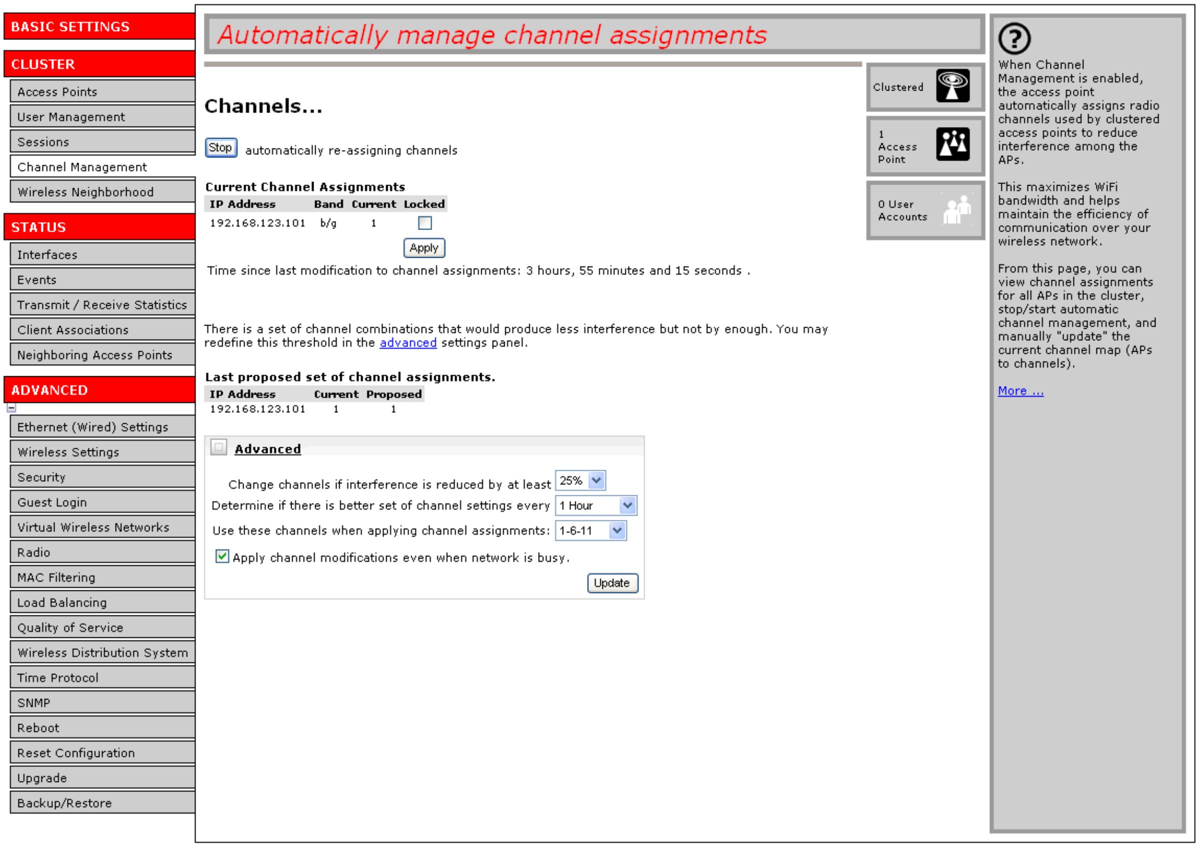
Channel Management

The following Channel Management topics are covered here:

- Navigating to Channel Management
- Understanding Channel Management
    - How it Works: Overview
    - Overlapping Channels: Background Information
    - Example: A Network before and after Channel Management
- Configuring and Viewing Channel Management Settings
    - Stopping/Starting Automatic Channel Assignment
    - Viewing Current Channel Assignments and Setting Locks
    - Viewing Last Proposed Set of Changes
    - Configuring Advanced Settings (Customizing and Scheduling Channel Plans)

Navigating to Channel Management

To view session monitoring information, click the Cluster menu’s **Channel Management** tab.



Automatically manage channel assignments

Channels...

Stop automatically re-assigning channels

Current Channel Assignments

IP Address	Band	Current	Locked
192.168.123.101	b/g	1	□

Apply

Time since last modification to channel assignments: 3 hours, 55 minutes and 15 seconds .

There is a set of channel combinations that would produce less interference but not by enough. You may redefine this threshold in the advanced settings panel.

Last proposed set of channel assignments.

IP Address	Current	Proposed
192.168.123.101	1	1

□ **Advanced**

Change channels if interference is reduced by at least 25%

Determine if there is better set of channel settings every 1 Hour

Use these channels when applying channel assignments: 1-6-11

☑ Apply channel modifications even when network is busy.

Update

When Channel Management is enabled, the access point automatically assigns radio channels used by clustered access points to reduce interference among the APs.

This maximizes WiFi bandwidth and helps maintain the efficiency of communication over your wireless network.

From this page, you can view channel assignments for all APs in the cluster, stop/start automatic channel management, and manually "update" the current channel map (APs to channels).

More ...

Understanding Channel Management

When Channel Management is enabled, the Professional Access Point automatically assigns radio channels used by clustered access points to reduce interference with access points both within and outside of its cluster. This dynamic channel assignment maximizes Wi-Fi bandwidth and helps maintain the efficiency of communication over your wireless network.

How it Works: Overview

At a specified interval, or on demand, Channel Management maps APs to channel use and measures interference levels in the cluster. If significant channel interference is detected, Channel Management automatically reassigns some or all of the APs to new channels according to an efficiency algorithm (or *automated channel plan*).

Overlapping Channels: Background Information

The radio frequency (RF) broadcast Channel defines the portion of the radio spectrum that the radio on the access point uses for transmitting and receiving. The range of available channels for an access point is determined by the IEEE 802.11 mode, or band, of the access point. IEEE 802.11b and 802.11g modes (802.11 b/g) support the use of channels 1 through 11.

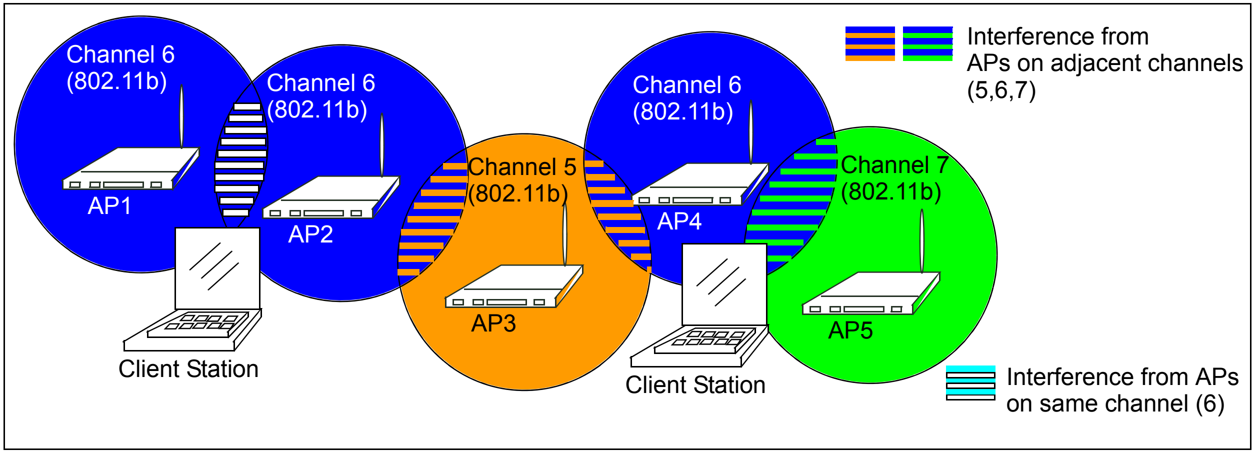
Interference can occur when multiple access points within range of each other are broadcasting on the same or overlapping channels. The impact of this interference on network performance can intensify during busy times when large amounts of data and media traffic compete for bandwidth.

Channel management uses a predetermined set of channels that minimizes interference. For the b/g radio band, the classic set of non-interfering channels is 1, 6, 11. Channels 1, 4, 8, 11 produce minimal overlap.

Example: A Network before and after Channel Management

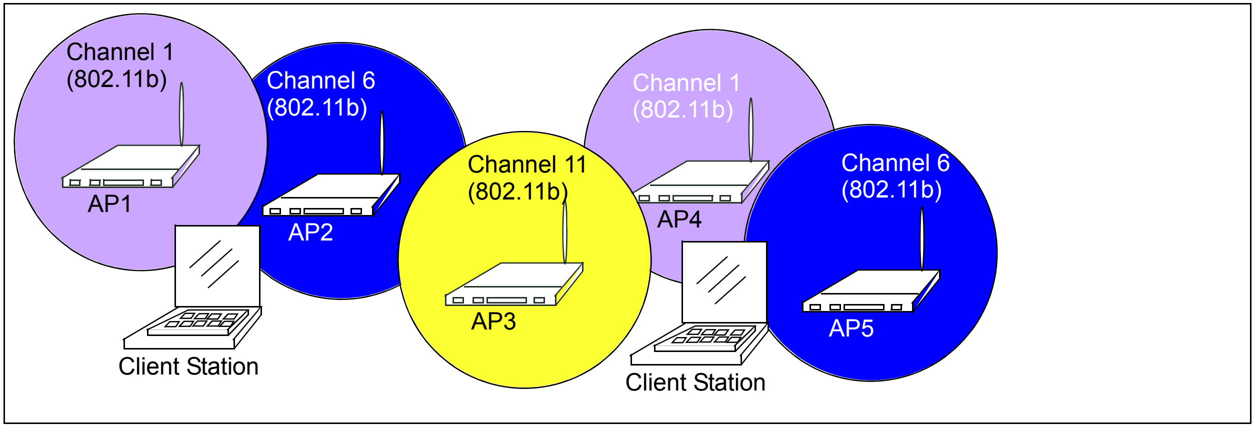
Without automated channel management, channel assignments to clustered APs might be made on consecutive channels, which would overlap and cause interference. For example, AP1 could be assigned to channel 6, AP2 to channel 6, and AP3 to channel 5 as shown in Figure 3.

Figure 3. Without Automatic Channel Management: APs Can Broadcast on Overlapping Channels.



With automated channel management, APs in the cluster are automatically reassigned to non-interfering channels as shown in Figure 4.

Figure 4. With Channel Management Enabled: APs are Reassigned to Non-Interfering Channels.



Configuring and Viewing Channel Management Settings

The Channel Management page shows previous, current, and planned channel assignments for clustered access points. By default, automatic channel assignment is disabled. You can start channel management to optimise channel usage across the cluster on a scheduled interval.

From this page, you can view channel assignments for all APs in the cluster, stop and start automatic channel management, and manually update the current channel map (APs to channels). During a manual update, channel management will assess channel usage and, if necessary, reassign APs to new channels to reduce interference based on the current Advanced channel management settings.

By using the Advanced channel management settings you can modify the interference reduction potential that triggers channel reassignment, change the schedule for automatic updates, and reconfigure the channel set used for assignments.

The following sections describe how to configure and use channel management on your network:

- Stopping/Starting Automatic Channel Assignment
- Viewing Current Channel Assignments and Setting Locks
    - Update Current Channel Assignments Manually
- Viewing Last Proposed Set of Changes
- Configuring Advanced Settings (Customizing and Scheduling Channel Plans)
    - Update Advanced Settings

Stopping/Starting Automatic Channel Assignment

By default, automatic channel assignment is disabled (off).

To enable automatic channel assignment,

1. Click **Start**.
2. Wait 60 seconds.
3. Use your browser control to refresh the Channel Management page.

   When automatic channel assignment is enabled, channel management periodically maps radio channels used by clustered access points and, if necessary, reassigns channels on clustered APs to reduce interference with either cluster members or APs outside the cluster.

   Note Channel Management overrides the default cluster behaviour, which is to synchronize radio channels of all APs across a cluster. When Channel Management is enabled, the radio Channel is not synchronized across the cluster to other APs. See the note under Radio Settings in “Settings Shared in the Cluster Configuration” on page 45.

To stop automatic channel assignment, click **Stop**. No channel usage maps or channel reassignments will be made. Only manual updates will affect the channel assignment.

Viewing Current Channel Assignments and Setting Locks

The **Current Channel Assignments** show a list of all access points in the cluster by IP Address. The display shows the band on which each access point is broadcasting, the channel currently used by each access point, and an option to lock an access point on its current radio channel so that it cannot be reassigned to another. Details about **Current Channel Assignments** are provided below.

Field	Description
IP Address	Specifies the IP Address for the access point.
Band	Indicates the band on which the access point is broadcasting.
Current	Indicates the radio Channel on which this access point is currently broadcasting.
Locked	Select **Locked** if you want to this access point to remain on the current channel. When an access point's channel is locked, automated channel management plans will not reassign the access point to a different channel as a part of the optimization strategy. Instead, APs with locked channels will be factored in as requirements for the plan. If you click **Apply**, you will see that locked APs show the same channel for **Current Channel** and **Proposed Channel**. Locked APs keep their current channels.

Update Current Channel Assignments Manually

You can run a manual channel management update at any time by clicking **Update** under the **Current Channel Assignments** display.

Viewing Last Proposed Set of Changes

The **Last Proposed Set of Channel Assignments** shows the last channel plan. The plan lists all access points in the cluster by IP Address and shows the current and proposed channels for each access point. Locked channels will not be reassigned, and the optimization of channel distribution among APs will take into account the fact that locked APs must remain on their current channels. APs that are not locked may be assigned to different channels than they were previously using, depending on the results of the plan.

Field	Description
IP Address	Specifies the IP Address for the access point.
Current	Indicates the radio channel on which this access point is currently broadcasting.
Proposed	Indicates the radio channel to which this access point would be reassigned if the Channel Plan is executed.

Configuring Advanced Settings (Customizing and Scheduling Channel Plans)

If you use channel management without updating Advanced settings, channels are automatically fine-tuned once every hour if interference can be reduced by 25 percent or more. Channels will be reassigned even if the network is busy. These defaults are designed to satisfy most situations in which you would need to implement channel management.

You can use **Advanced** settings to modify the interference reduction potential that triggers channel reassignment, change the schedule for automatic updates, and reconfigure the channel set used for assignments

Field	Description
Advanced	Click **Advanced** to show or hide display settings that modify timing and details of the channel planning algorithm. By default, advanced settings are hidden.
Change channels if interference is reduced by at least	Specify the minimum percentage of interference reduction a proposed plan must achieve in order to be applied. The default is 25 percent. Use the list to select percentages ranging from 5 percent to 75 percent. This setting lets you set a gating factor for channel reassignment so that the network is not continually disrupted for minimal gains in efficiency. For example, if channel interference must be reduced by 75 percent and the proposed channel assignments will only reduce interference by 30 percent, then channels will not be reassigned. However; if you reset the minimal channel interference benefit to 25 percent and click **Update**, the proposed channel plan will be implemented and channels reassigned as needed.
Determine if there is better set of channels every	Specify the schedule for automated updates. A range of intervals is provided, from 1 minute to 6 months The default is 1 hour (channel usage assessed and the resulting channel plan applied every hour).
Use these channels when applying channel assignments	Choose a set of non-interfering channels. The choices are: • b/g channels 1-6-11 • b/g channels 1-4-8-11 IEEE 802.11b and 802.11g modes support use of channels 1 through 11. For b and g radio bands, the classic set of non-interfering channels is 1, 6, and 11. Channels 1, 4, 8, and 11 produce minimal overlap.

Field	Description
Apply channel modifications even when the network is busy	Click to enable or disable this setting. If you enable this setting, channel modifications will be applied even when the network is busy. If you disable this setting, channel modifications will not be applied on a busy network. This setting, along with the interference reduction setting, is designed to help weigh the cost/benefit impact on network performance of reassigning channels against the inherent disruption it can cause to clients during a busy time.

Update Advanced Settings

Click **Update** under **Advanced** settings to apply these settings.

Advanced settings take affect when they are applied, and they influence how automatic channel management is performed. The new interference reduction minimum, scheduled tuning interval, channel set, and network busy settings will be taken into account for automated and manual updates.

Wireless Neighborhood

The Wireless Neighborhood view shows those access points within range of any access point in the cluster. This page provides a detailed view of neighbouring access points including identifying information such as SSIDs and MAC addresses for each, cluster status, and statistical information such as the broadcast channel and signal strength of each AP.

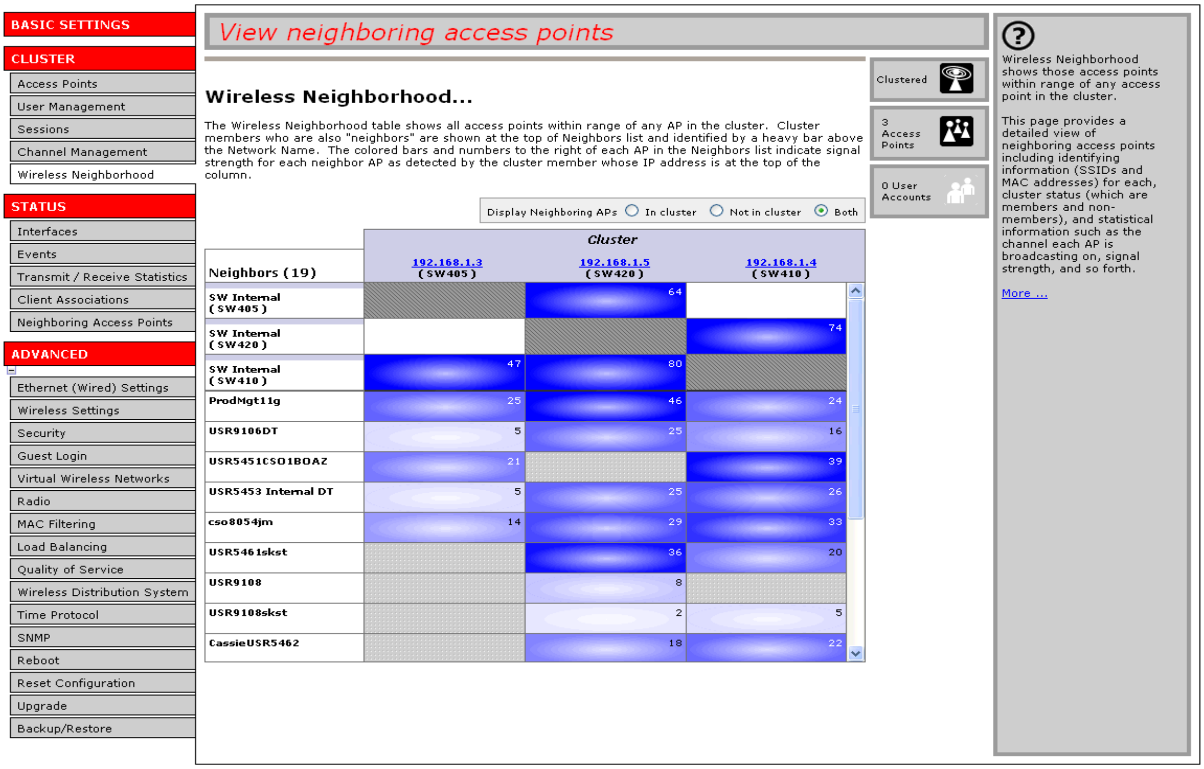
The following topics are covered here:

- Navigating to Wireless Neighborhood
- Understanding Wireless Neighbourhood Information
- Viewing Wireless Neighborhood
- Viewing Details for a Cluster Member

Navigating to Wireless Neighborhood

To view the Wireless Neighborhood, click the Cluster menu's **Wireless Neighborhood** tab.

Figure 5. Neighbour APs Both in Cluster and Not in Cluster.



View neighboring access points

Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighbor AP as detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs ○ In cluster ○ Not in cluster ● Both

	Cluster		
Neighbors (19)	192.168.1.3 (SW405)	192.168.1.5 (SW420)	192.168.1.4 (SW410)
SW Internal (SW405)	▨	64	
SW Internal (SW420)		▨	74
SW Internal (SW410)	47	80	▨
ProdMgt11g	25	46	24
USR9106DT	5	25	16
USR5451CSO1BOAZ	21		39
USR5453 Internal DT	5	25	26
cso8054jm	14	29	33
USR5461skst		36	20
USR9108		8	
USR9108skst		2	5
CassieUSR5462		18	22

Wireless Neighborhood shows those access points within range of any access point in the cluster.

This page provides a detailed view of neighboring access points including identifying information (SSIDs and MAC addresses) for each, cluster status (which are members and non-members), and statistical information such as the channel each AP is broadcasting on, signal strength, and so forth.

Understanding Wireless Neighbourhood Information

The Wireless Neighborhood view shows all access points within range of every member of the cluster, shows which access points are within range of which cluster members, and distinguishes between cluster members and non-members.

For each neighbour access point, the Wireless Neighborhood view shows identifying information (SSID or Network Name, IP Address, MAC address) along with radio statistics (signal strength, channel, beacon interval). You can click on an access point's IP address to get additional statistics about the APs within radio range of the currently selected AP.

The Wireless Neighborhood view can help you:

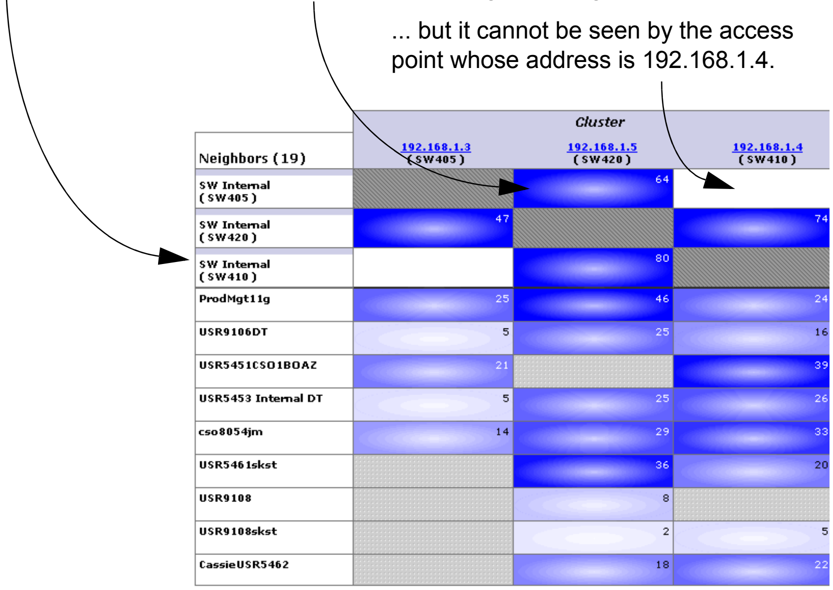
- Detect and locate unexpected (or *rogue*) access points in a wireless domain so that you can take action to limit associated risks.
- Verify coverage expectations. By assessing which APs are visible at what signal strength from other APs, you can verify that the deployment meets your planning goals.

- Detect faults. Unexpected changes in the coverage pattern are evident at a glance in the colour coded table.

Viewing Wireless Neighborhood

Details about Wireless Neighborhood information shown is described below.

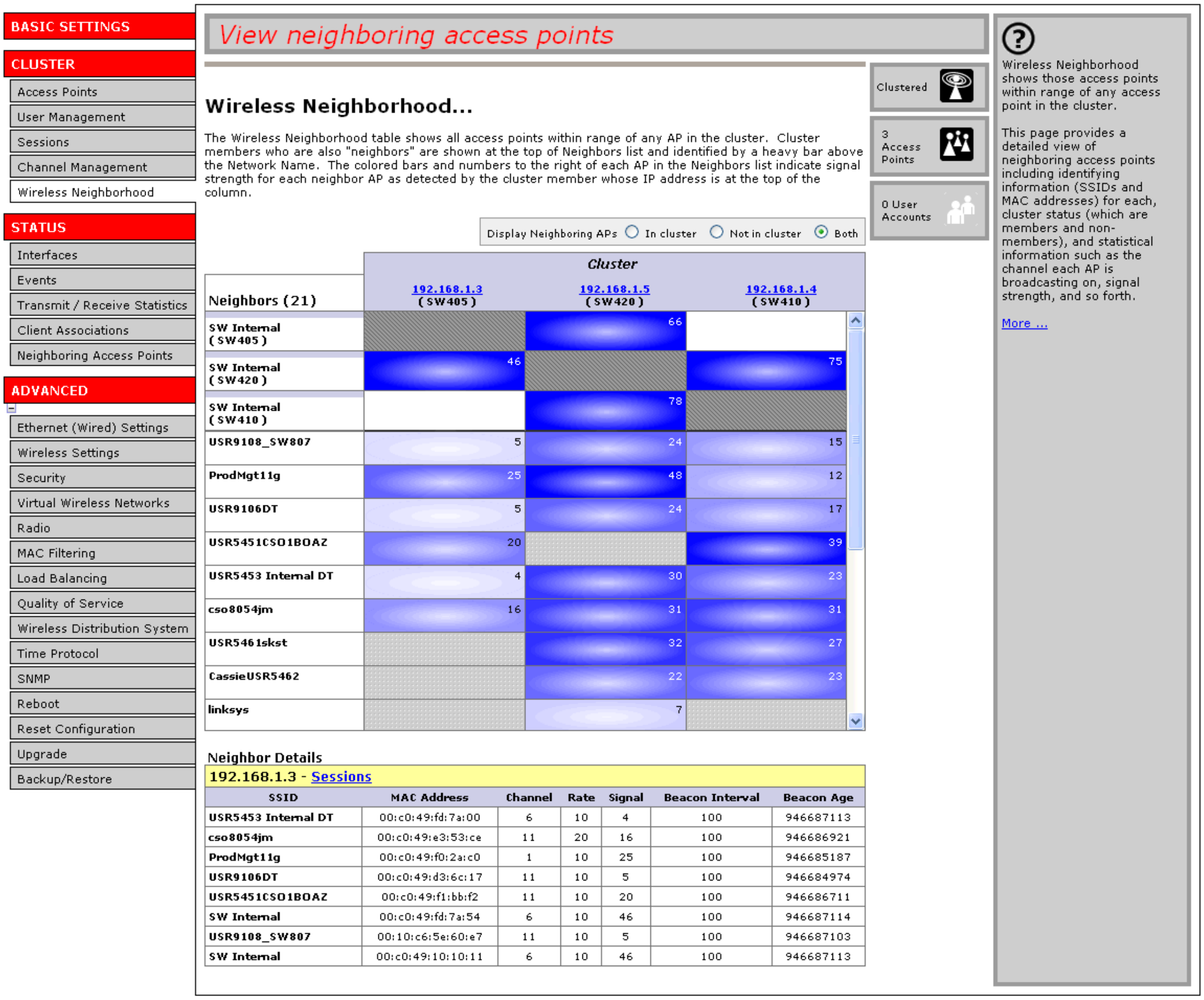
Field	Description
Display neighboring APs	Click one of the following radio buttons to change the view: • **In cluster** - Shows only neighbour APs that are members of the cluster • **Not in cluster** - Shows only neighbour APs that are not cluster members • **Both** - Shows all neighbour APs (cluster members and non-members)
Cluster	The **Cluster** list at the top of the table shows IP addresses for all access points in the cluster. This is the same list of cluster members shown on the Cluster menu's Access Points tab described in "Navigating to Access Points Management" on page 44. If there is only one AP in the cluster, only a single IP address column will be displayed here; indicating that the AP is clustered with itself. You can click an IP address to view more details for a particular AP as shown in Figure 6 below.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><b>Neighbors</b></td><td>
<p>Access points that are neighbours of one or more of the clustered APs are listed in the left column by SSID (Network Name).</p>
<p>An access point which is detected as a neighbour of a cluster member can also be a cluster member itself. Neighbours who are also cluster members are always shown at the top of the list with a heavy bar above the name and include a location indicator.</p>
<p>The coloured bars to the right of each AP in the Neighbors list shows the signal strength for each of the neighbour APs as detected by the cluster member whose IP address is shown at the top of the column:</p>
<p>This access point is a cluster member and can be seen by the AP whose IP address is 192.168.1.5 at a signal strength of 64...</p>
<p>... but it cannot be seen by the access point whose address is 192.168.1.4.</p>

<table>
<tr><th></th><th colspan="3"><i>Cluster</i></th></tr>
<tr><th>Neighbors (19)</th><th>192.168.1.3
(SW405)</th><th>192.168.1.5
(SW420)</th><th>192.168.1.4
(SW410)</th></tr>
<tr><td>SW Internal
(SW405)</td><td>▨</td><td>64</td><td></td></tr>
<tr><td>SW Internal
(SW420)</td><td>47</td><td>▨</td><td>74</td></tr>
<tr><td>SW Internal
(SW410)</td><td></td><td>80</td><td>▨</td></tr>
<tr><td>ProdMgt11g</td><td>25</td><td>46</td><td>24</td></tr>
<tr><td>USR9106DT</td><td>5</td><td>25</td><td>16</td></tr>
<tr><td>USR5451CSO1BOAZ</td><td>21</td><td>░</td><td>39</td></tr>
<tr><td>USR5453 Internal DT</td><td>5</td><td>25</td><td>26</td></tr>
<tr><td>cso8054jm</td><td>14</td><td>29</td><td>33</td></tr>
<tr><td>USR5461skst</td><td>░</td><td>36</td><td>20</td></tr>
<tr><td>USR9108</td><td>░</td><td>8</td><td>░</td></tr>
<tr><td>USR9108skst</td><td>░</td><td>2</td><td>5</td></tr>
<tr><td>CassieUSR5462</td><td>░</td><td>18</td><td>22</td></tr>
</table>
<ul>
<li><b>Dark Blue Bar</b> - A dark blue bar and a high signal strength number (for example 50) indicates good signal strength from the neighbour as seen by the AP whose IP address is shown at the top of the column.</li>
<li><b>Lighter Blue Bar -</b> A lighter blue bar and a lower signal strength number (for example 20 or lower) indicates medium or weak signal strength from the neighbour as seen by the AP whose IP address is shown at the top of the column.</li>
<li><b>White Bar</b> - A white bar and the number 0 indicates that a neighbouring AP that was detected by one of the cluster members cannot be detected by the AP whose IP address is shown at the top of the column.</li>
<li><b>Light Gray Bar -</b> A light gray bar and no signal strength number indicates a neighbour that is detected by other cluster members but not by the AP whose IP address is shown at the top of the column.</li>
<li><b>Dark Gray Bar</b> - A dark gray bar and no signal strength number indicates this <i>is</i> the AP whose IP address is shown at the top of the column.</li>
</ul>
</td></tr>
</table>

Viewing Details for a Cluster Member

To view details on a cluster member AP, click the IP address of a cluster member at the top of the table.

Figure 6. Details for a Cluster Member AP.



View neighboring access points

Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighbor AP as detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs ○ In cluster ○ Not in cluster ● Both

	Cluster		
Neighbors (21)	192.168.1.3 (SW405)	192.168.1.5 (SW420)	192.168.1.4 (SW410)
SW Internal (SW405)		66	
SW Internal (SW420)	46		75
SW Internal (SW410)		78	
USR9108_SW807	5	24	15
ProdMgt11g	25	48	12
USR9106DT	5	24	17
USR5451CSO1BOAZ	20		39
USR5453 Internal DT	4	30	23
cso8054jm	16	31	31
USR5461skst		32	27
CassieUSR5462		22	23
linksys		7	

Neighbor Details

192.168.1.3 - Sessions

SSID	MAC Address	Channel	Rate	Signal	Beacon Interval	Beacon Age
USR5453 Internal DT	00:c0:49:fd:7a:00	6	10	4	100	946687113
cso8054jm	00:c0:49:e3:53:ce	11	20	16	100	946686921
ProdMgt11g	00:c0:49:f0:2a:c0	1	10	25	100	946685187
USR9106DT	00:c0:49:d3:6c:17	11	10	5	100	946684974
USR5451CSO1BOAZ	00:c0:49:f1:bb:f2	11	10	20	100	946686711
SW Internal	00:c0:49:fd:7a:54	6	10	46	100	946687114
USR9108_SW807	00:10:c6:5e:60:e7	11	10	5	100	946687103
SW Internal	00:c0:49:10:10:11	6	10	46	100	946687113

Wireless Neighborhood shows those access points within range of any access point in the cluster.

This page provides a detailed view of neighboring access points including identifying information (SSIDs and MAC addresses) for each, cluster status (which are members and non-members), and statistical information such as the channel each AP is broadcasting on, signal strength, and so forth.

More ...

The following table explains the details shown about the selected AP.

Field	Description
SSID	Shows the *Service Set Identifier* (SSID) for the access point. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. The SSID is set in Basic Settings. (See “Basic Settings” on page 35) or on Advanced menu’s Wireless Settings page (see “Wireless Settings” on page 97.) A Guest network and an Internal network running on the same access point must always have two different network names.
MAC Address	Shows the MAC address of the neighbouring access point. A MAC address is a hardware address that uniquely identifies each node of a network.
Channel	Shows the channel on which the access point is currently broadcasting. The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The channel is set on the Advanced menu’s Radio Settings page. (See “Radio” on page 129.)
Rate	Shows the rate (in megabits per second) at which this access point is currently transmitting. The current rate will always be one of the rates shown in Supported Rates.
Signal	Indicates the strength of the radio signal emitting from this access point as measured in decibels (Db).
Beacon Interval	Shows the Beacon interval being used by this access point. Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behaviour is to send a beacon frame once every 100 milliseconds (or 10 per second). The beacon Interval is set on the Advanced menu’s Radio Settings page. (See “Radio” on page 129.)
Beacon Age	Shows the date and time of the most recent beacon transmission from the access point.

Status

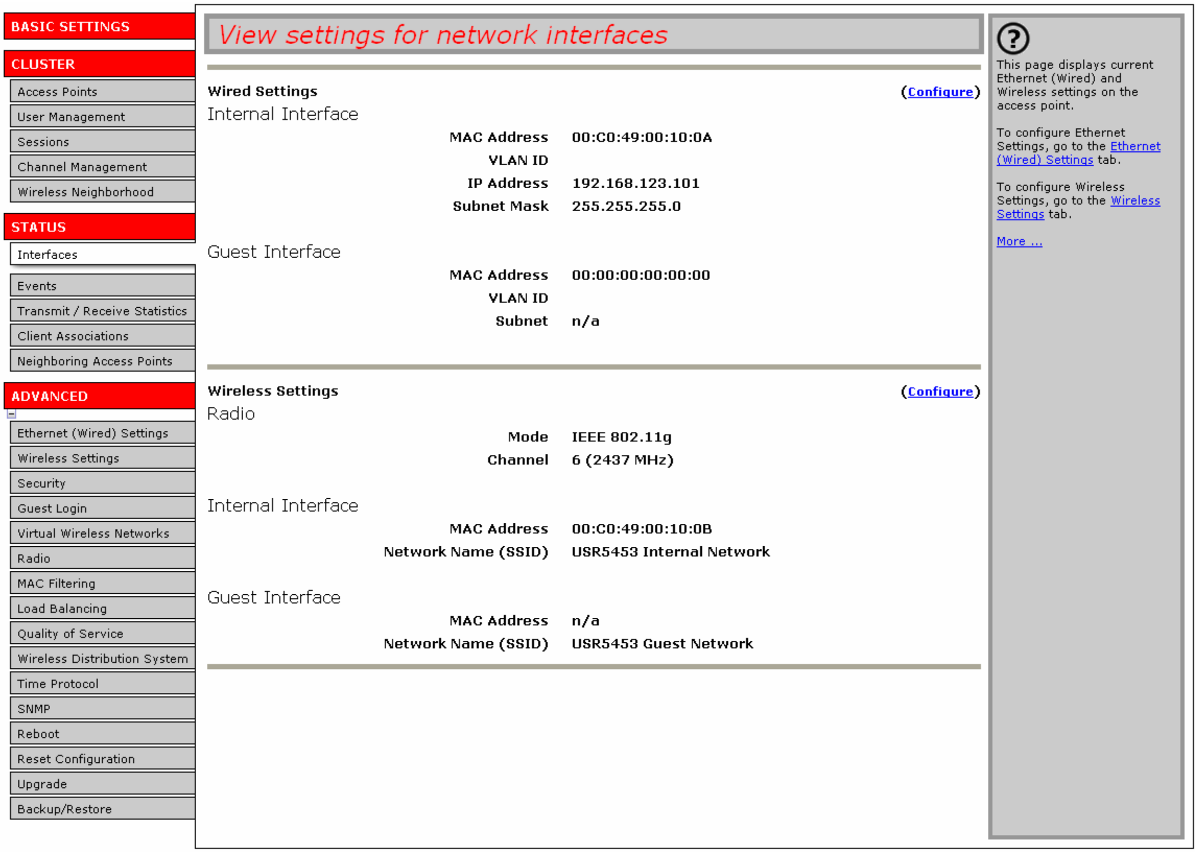
You can view information about an individual access point from the Status menu. Because the Status pages display settings for a specific access point—not for a cluster configuration that is automatically shared by multiple access points—it is important to ensure that you are accessing the Web User Interface for the access point that you want to monitor (see “Navigating to the Web User Interface for a Specific Access Point” on page 50.)

You can use the Status pages to monitor the following aspects of an access point:

- Interfaces
- Events
- Transmit/Receive Statistics
- Client Associations
- Neighboring Access Points

Interfaces

To monitor wired LAN and wireless LAN (WLAN) settings, navigate to the Status menu’s **Interfaces** tab on the Web User Interface for the access point that you want to monitor.



View settings for network interfaces

Wired Settings

Internal Interface

MAC Address	00:C0:49:00:10:0A
VLAN ID	
IP Address	192.168.123.101
Subnet Mask	255.255.255.0

Guest Interface

MAC Address	00:00:00:00:00:00
VLAN ID	
Subnet	n/a

Wireless Settings

Radio

Mode	IEEE 802.11g
Channel	6 (2437 MHz)

Internal Interface

MAC Address	00:C0:49:00:10:0B
Network Name (SSID)	USR5453 Internal Network

Guest Interface

MAC Address	n/a
Network Name (SSID)	USR5453 Guest Network

This page displays current Ethernet (Wired) and Wireless settings on the access point.

To configure Ethernet Settings, go to the Ethernet (Wired) Settings tab.

To configure Wireless Settings, go to the Wireless Settings tab.

This page displays the current **Ethernet (Wired) Settings** and **Wireless Settings**.

Ethernet (Wired) Settings

The Internal interface includes the Ethernet MAC Address, VLAN ID, IP Address, and Subnet Mask.

The Guest interface includes the MAC Address, VLAN ID, and Subnet.

If you want to change any of these settings, click the **Configure** link.

Wireless Settings

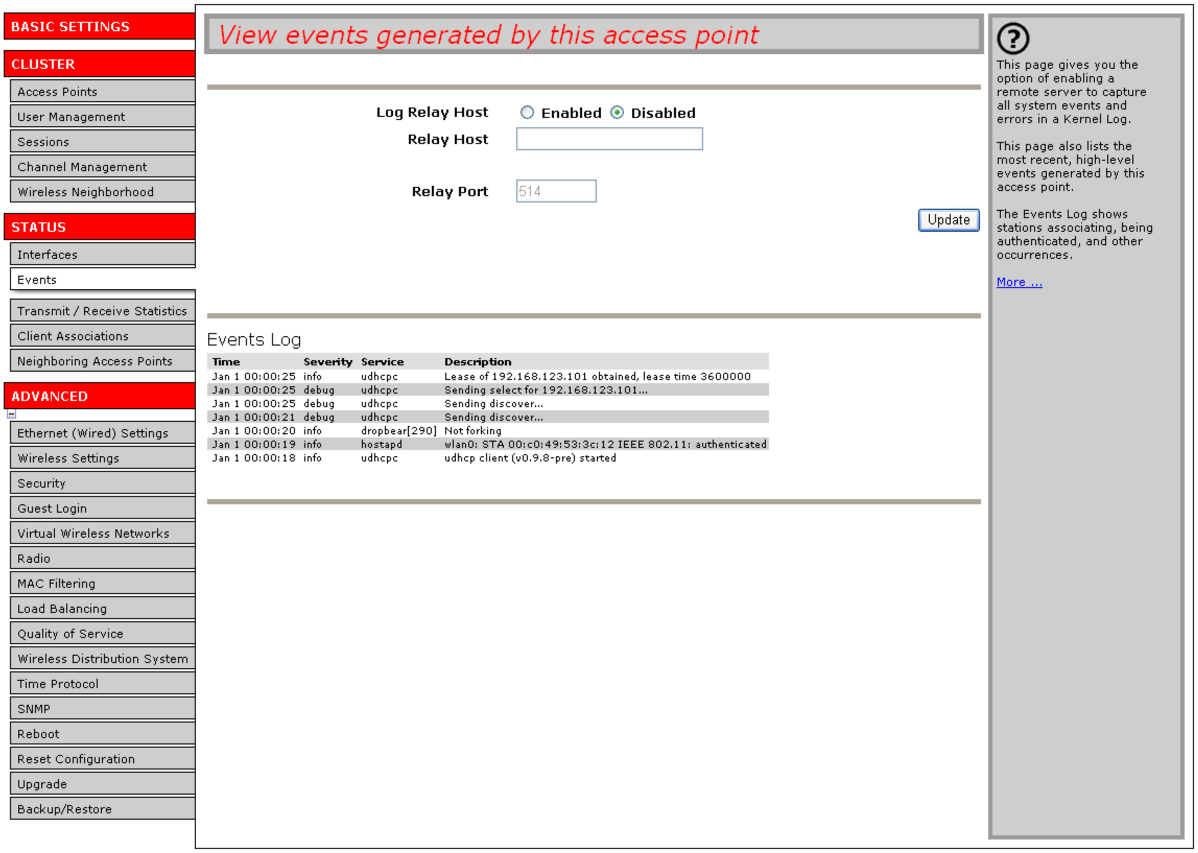
The Radio Interface settings include radio Mode and Channel. Also shown here are MAC addresses and network names for internal and guest interfaces. (See “Wireless Settings” on page 97 and “Radio” on page 129 for more information.)

If you want to change any of these settings, click the **Configure** link.

Events

To view system events and kernel log for a particular access point, navigate to the Status menu's **Events** tab on the Web User Interface for the access point that you want to monitor

.



View events generated by this access point

Log Relay Host ○ Enabled ● Disabled

Relay Host

Relay Port 514

Events Log

Time	Severity	Service	Description
Jan 1 00:00:25	info	udhcpc	Lease of 192.168.123.101 obtained, lease time 3600000
Jan 1 00:00:25	debug	udhcpc	Sending select for 192.168.123.101...
Jan 1 00:00:25	debug	udhcpc	Sending discover...
Jan 1 00:00:21	debug	udhcpc	Sending discover...
Jan 1 00:00:20	info	dropbear[290]	Not forking
Jan 1 00:00:19	info	hostapd	wlan0: STA 00:c0:49:53:3c:12 IEEE 802.11: authenticated
Jan 1 00:00:18	info	udhcpc	udhcp client (v0.9.8-pre) started

This page gives you the option of enabling a remote server to capture all system events and errors in a Kernel Log.

This page also lists the most recent, high-level events generated by this access point.

The Events Log shows stations associating, being authenticated, and other occurrences.

This page lists the most recent events generated by this access point (see "Events Log" on page 82).

This page also gives you the option of enabling a remote log relay host to capture all system events and errors in a Kernel Log. (This requires setting up a remote relay host first. See "Log Relay Host for Kernel Messages" on page 79).

Note

The Professional Access Point acquires its date and time information using the network time protocol (NTP). This data is reported in UTC format (also known as *Greenwich Mean Time*). You need to convert the reported time to your local time.

For information on setting the network time protocol, see "Time Protocol" on page 161.

Log Relay Host for Kernel Messages

- Understanding Remote Logging
- Setting Up the Log Relay Host

- Enabling and Disabling the Log Relay Host on the Status Menu’s Events Page

Understanding Remote Logging

The *kernel log* is a comprehensive list of system events (shown in the System Log) and kernel messages, such as an error message for dropping frames.

You cannot view kernel log messages directly from the Web User Interface for an access point. You must first set up a remote server running a syslog process and acting as a system log relay host on your network. Then, you can configure the Professional Access Point to send its system log messages to the remote server.

Using a remote server to collect access point system log messages affords you several benefits. You can:

- Aggregate system log messages from multiple access points
- Store a longer history of messages than kept on a single access point
- Trigger scripted management operations and alerts

Setting Up the Log Relay Host

To use kernel log relaying, you must configure a remote server to receive the syslog messages. This procedure will vary depending on the type of machine you use as the remote log host. Following is an example of how to configure a remote Linux server using the syslog daemon.

Example of Using Linux syslogd

The following steps activate the syslog daemon on a Linux server. Make sure that you have `root` user identity for these tasks.

1. Log on as `root` to the machine that you want to use as your syslog relay host.

   The following operations require `root` user permissions. If you are not already logged on as `root`, type `su` at the command line prompt to become `root` ("super user").

2. Edit `/etc/init.d/sysklogd` and add "`-r`" to the variable `SYSLOGD` near the top of the file. The line that you edit will look like this:

   ```
   SYSLOGD="-r"
   ```

   Consult the man pages to get more information on `syslogd` command options. (Type `man syslogd` at the command line.)

3. If you want to send all the messages to a file, edit `/etc/syslog.conf`.

   For example you can add this line to send all messages to a log file called *`AP_syslog`*:

   ```
   *.*        -/tmp/AP_syslog
   ```

   Consult the `man` pages to get more information on `syslog.conf` command options. (Type `man syslog.conf` at the command line.)

4. Restart the syslog server by typing the following at the command line prompt:

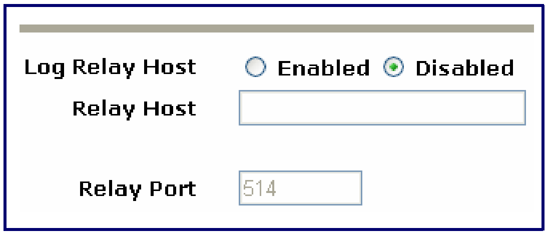
```
/etc/init.d/sysklogd restart
```

Note The syslog process will default to use port 514. USRobotics recommends using this default port.

However, if you choose to reconfigure the log port, make sure that the port number that you assign to syslog is not being used by another process.

Enabling and Disabling the Log Relay Host on the Status Menu's Events Page

To enable and configure log relaying on the Status menu's **Events** page, set the log relay options as described below.



Log Relay Host ○ Enabled ● Disabled

Relay Host

Relay Port 514

Field	Description
Log Relay Host Enabled	Choose to either enable or disable use of the Log Relay Host: • **Enabled** • **Disabled** If you select **Enabled**, the **Relay Host** and **Relay Port** fields are editable.
Relay Host	Specify the IP Address or DNS name of the relay host.
Relay Port	Specify the port number for the syslog process on the relay host. The default port is 514.

Update Settings

To apply your changes, click **Update**.

If you enabled the log relay host, clicking **Update** will activate remote logging. The access point will send its kernel messages real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on how you configured the log relay host.

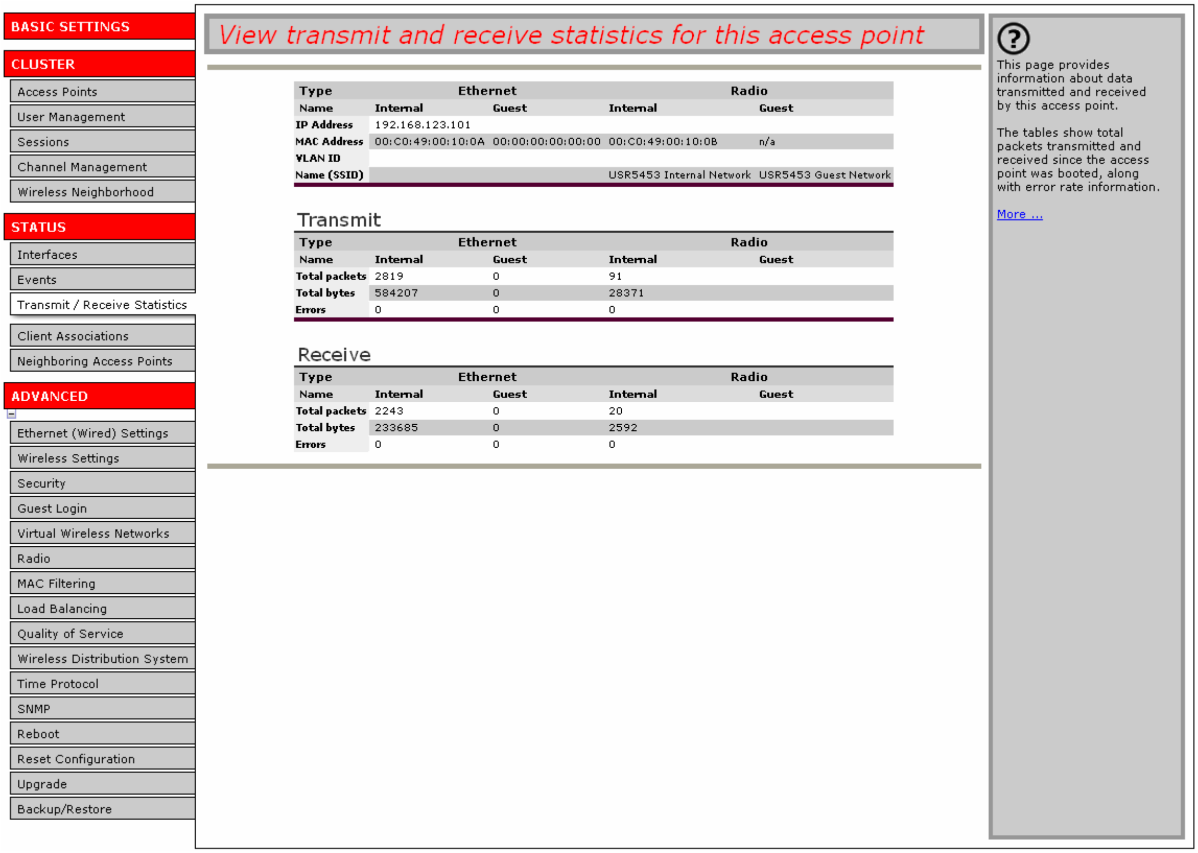
If you disabled the log relay host, clicking **Update** will disable remote logging.

Events Log

The Events Log shows system events on the access point such as stations associating or being authenticated. The real-time Events Log is always shown on the Status menu's Events page for the access point you are monitoring.

Transmit/Receive Statistics

To view transmit/receive statistics for a particular access point, navigate to the Status menu's **Transmit/ Receive Statistics** on the Web User Interface for the access point that you want to monitor.



View transmit and receive statistics for this access point

Type	Ethernet		Radio	
Name	Internal	Guest	Internal	Guest
IP Address	192.168.123.101			
MAC Address	00:C0:49:00:10:0A	00:00:00:00:00:00	00:C0:49:00:10:0B	n/a
VLAN ID				
Name (SSID)			USR5453 Internal Network	USR5453 Guest Network

Transmit

Type	Ethernet		Radio	
Name	Internal	Guest	Internal	Guest
Total packets	2819	0	91	
Total bytes	584207	0	28371	
Errors	0	0	0	

Receive

Type	Ethernet		Radio	
Name	Internal	Guest	Internal	Guest
Total packets	2243	0	20	
Total bytes	233685	0	2592	
Errors	0	0	0	

This page provides information about data transmitted and received by this access point.

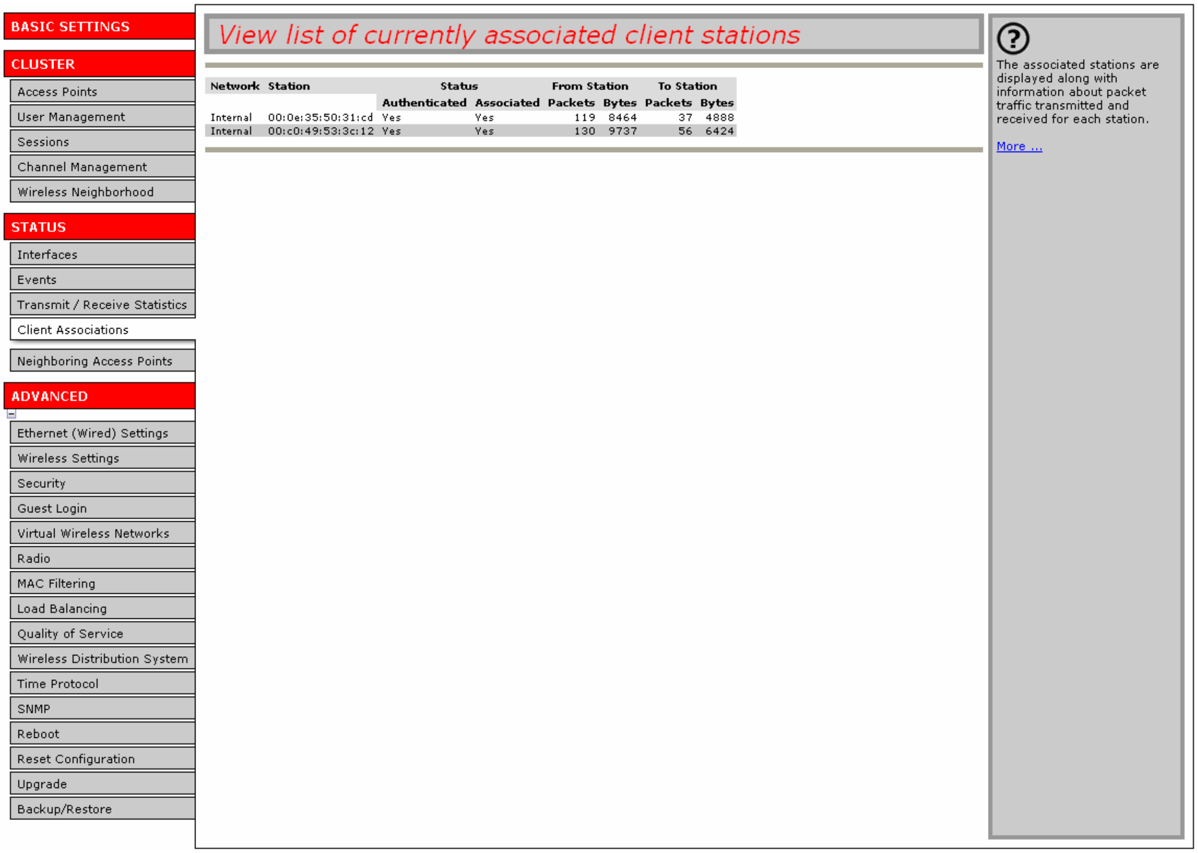
The tables show total packets transmitted and received since the access point was booted, along with error rate information.

This page provides basic information about the current access point and a real-time display of the transmit and receive statistics for this access point as described in the table below. All transmit and receive statistics shown are totals accumulated since the access point was last started. If the access point is rebooted, these figures indicate transmit/receive totals since the reboot.

Field	Description
IP Address	IP Address for the access point.
MAC Address	Media Access Control (MAC) address for the specified interface. The Professional Access Point has a unique MAC address for each interface.
VLAN ID	Virtual LAN (VLAN) ID. A VLAN is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. VLANs can be used to establish internal and guest networks on the same access point.
Name (SSID)	Wireless network name. Also known as the *SSID*, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the Basic Settings tab. (See “Provide Administrator Password and Wireless Network Name” on page 38.)
Transmit and Receive Information	
Total Packets	The total count of packets sent (in the **Transmit** table) or received (in the **Received** table) by this access point.
Total Bytes	The total count of bytes sent (in the **Transmit** table) or received (in the **Received** table) by this access point.
Errors	The total count of errors related to sending and receiving data on this access point.

Client Associations

To view the client stations associated with a particular access point, navigate to the Status menu’s **Client Associations** on the Web User Interface for the access point that you want to monitor.



View list of currently associated client stations

Network	Station	Status		From Station		To Station	
		Authenticated	Associated	Packets	Bytes	Packets	Bytes
Internal	00:0e:35:50:31:cd	Yes	Yes	119	8464	37	4888
Internal	00:c0:49:53:3c:12	Yes	Yes	130	9737	56	6424

The associated stations are displayed along with information about packet traffic transmitted and received for each station.

The associated stations are displayed along with information about packet traffic transmitted and received for each station.

Link Integrity Monitoring

The Professional Access Point provides *link integrity monitoring* to continually verify the access point's connection to each associated client, even when no data exchange is occurring. To perform this verification, the access point sends data packets to clients every few seconds when no other traffic is passing. This allows the access point to detect a client's having gone out of range, even during periods when no normal traffic is exchanged.The client connection is dropped from the list of associated clients within 300 seconds of the client disappearing, even if the client does not disassociate (but went out of range).

What is the Difference Between an Association and a Session?

An *association* describes a client's connection to a particular access point. A *session* describes a client's connection to the network. A client's network connection can shift from one clustered access point to another within the context of the same session. A client station can roam between APs and maintain the session.

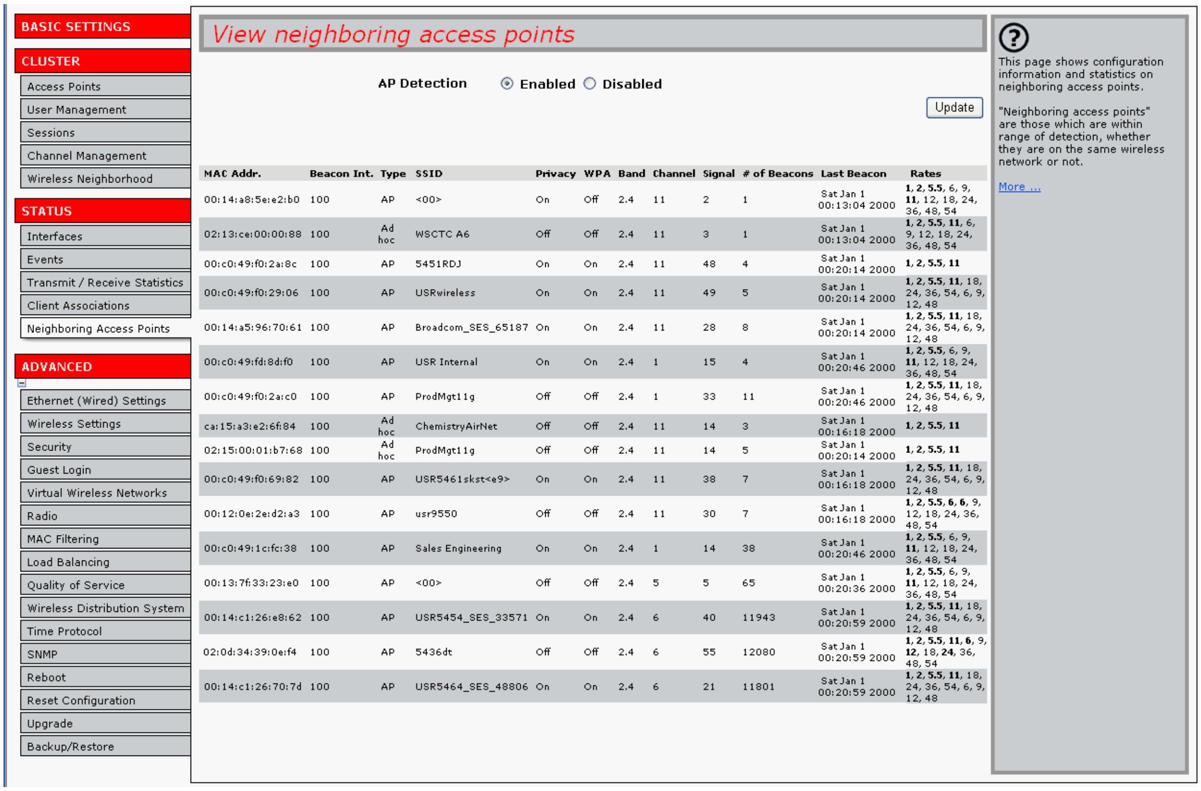
For information on monitoring *sessions*, see "Understanding Session Monitoring Information" on page 60.

Neighboring Access Points

The status page for neighbouring access points provides real-time statistics for all access points within range of the access point on which you are viewing the Web User Interface.

To view information about other access points on the wireless network,

1. Navigate to the Status menu’s **Neighboring Access Points** tab.



View neighboring access points

AP Detection ◉ Enabled ○ Disabled

MAC Addr.	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Signal	# of Beacons	Last Beacon	Rates
00:14:a8:5e:e2:b0	100	AP	<00>	On	Off	2.4	11	2	1	Sat Jan 1 00:13:04 2000	**1**, **2**, **5.5**, 6, 9, **11**, 12, 18, 24, 36, 48, 54
02:13:ce:00:00:88	100	Ad hoc	WSCTC A6	Off	Off	2.4	11	3	1	Sat Jan 1 00:13:04 2000	**1**, **2**, **5.5**, **11**, 6, 9, 12, 18, 24, 36, 48, 54
00:c0:49:f0:2a:8c	100	AP	5451RDJ	On	On	2.4	11	48	4	Sat Jan 1 00:20:14 2000	**1**, **2**, **5.5**, **11**
00:c0:49:f0:29:06	100	AP	USRwireless	On	On	2.4	11	49	5	Sat Jan 1 00:20:14 2000	**1**, **2**, **5.5**, **11**, 18, 24, 36, 54, 6, 9, 12, 48
00:14:a5:96:70:61	100	AP	Broadcom_SES_65187	On	On	2.4	11	28	8	Sat Jan 1 00:20:14 2000	**1**, **2**, **5.5**, **11**, 18, 24, 36, 54, 6, 9, 12, 48
00:c0:49:fd:8d:f0	100	AP	USR Internal	On	On	2.4	1	15	4	Sat Jan 1 00:20:46 2000	**1**, **2**, **5.5**, 6, 9, **11**, 12, 18, 24, 36, 48, 54
00:c0:49:f0:2a:c0	100	AP	ProdMgt11g	Off	Off	2.4	1	33	11	Sat Jan 1 00:20:46 2000	**1**, **2**, **5.5**, **11**, 18, 24, 36, 54, 6, 9, 12, 48
ca:15:a3:e2:6f:84	100	Ad hoc	ChemistryAirNet	Off	Off	2.4	11	14	3	Sat Jan 1 00:16:18 2000	**1**, **2**, **5.5**, **11**
02:15:00:01:b7:68	100	Ad hoc	ProdMgt11g	Off	Off	2.4	11	14	5	Sat Jan 1 00:20:14 2000	**1**, **2**, **5.5**, **11**
00:c0:49:f0:69:82	100	AP	USR5461skst<e9>	On	On	2.4	11	38	7	Sat Jan 1 00:16:18 2000	**1**, **2**, **5.5**, **11**, 18, 24, 36, 54, 6, 9, 12, 48
00:12:0e:2e:d2:a3	100	AP	usr9550	Off	Off	2.4	11	30	7	Sat Jan 1 00:16:18 2000	**1**, **2**, **5.5**, **6**, **6**, 9, 12, 18, 24, 36, 48, 54
00:c0:49:1c:fc:38	100	AP	Sales Engineering	On	On	2.4	1	14	38	Sat Jan 1 00:20:46 2000	**1**, **2**, **5.5**, 6, 9, **11**, 12, 18, 24, 36, 48, 54
00:13:7f:33:23:e0	100	AP	<00>	Off	Off	2.4	5	5	65	Sat Jan 1 00:20:36 2000	**1**, **2**, **5.5**, 6, 9, **11**, 12, 18, 24, 36, 48, 54
00:14:c1:26:e8:62	100	AP	USR5454_SES_33571	On	On	2.4	6	40	11943	Sat Jan 1 00:20:59 2000	**1**, **2**, **5.5**, **11**, 18, 24, 36, 54, 6, 9, 12, 48
02:0d:34:39:0e:f4	100	AP	5436dt	Off	Off	2.4	6	55	12080	Sat Jan 1 00:20:59 2000	**1**, **2**, **5.5**, **11**, **6**, 9, **12**, 18, **24**, 36, 48, 54
00:14:c1:26:70:7d	100	AP	USR5464_SES_48806	On	On	2.4	6	21	11801	Sat Jan 1 00:20:59 2000	**1**, **2**, **5.5**, **11**, 18, 24, 36, 54, 6, 9, 12, 48

This page shows configuration information and statistics on neighboring access points.

"Neighboring access points" are those which are within range of detection, whether they are on the same wireless network or not.

2. Select **AP Detection Enabled**.

3. Click **Update**.

Information provided for neighbouring access points is described in the following table:

Field	Description
MAC Address	Shows the MAC address of the neighbouring access point. A MAC address is a hardware address that uniquely identifies each node of a network.
Beacon Int.	Shows the Beacon interval being used by this access point. Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behaviour is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval is set on Advanced menu's Radio Settings page. (See "Radio" on page 129.)
Type	Indicates the type of device: • **AP** indicates the neighbouring device is an access point that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode. • **Ad hoc** indicates a neighbouring station running in Ad-hoc Mode. Stations set to ad-hoc mode communicate with each other directly, without the use of a traditional access point. Ad-hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as *peer-to-peer* mode or an *Independent Basic Service Set* (IBSS).
SSID	The *Service Set Identifier* (SSID) for the access point. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. The SSID is set in Basic Settings (see "Basic Settings" on page 35) or on the Advanced menu's Wireless Settings page (see "Wireless Settings" on page 97). A Guest network and an Internal network running on the same access point must always have two different network names.
Privacy	Indicates whether there is any security on the neighbouring device. • **Off** indicates that the Security mode on the neighbouring device is set to **None** (no security). • **On** indicates that the neighbouring device has security in place. Access point security is configured on the Advanced menu's Security page. For more information on security settings, see "Security" on page 101.
WPA	Indicates whether WPA security is on or off for this access point.
Band	Indicates the IEEE 802.11 mode being used on this access point (IEEE 802.11b or IEEE 802.11g).

Field	Description
Channel	Shows the channel on which the access point is currently broadcasting. The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The channel is set on the Advanced menu’s Radio Settings page. (See “Radio” on page 129.)
Signal	Indicates the strength of the radio signal emitting from this access point as measured in decibels (Db).
# of Beacons	Shows the total number of beacons transmitted by this access point since the access point was last booted.
Last Beacon	Shows the date and time of the most recent beacon transmission from the access point.
Rates	Shows supported and basic (advertised) rate sets for the neighbouring access point. Rates are shown in megabits per second (Mbps). All supported rates are listed, with basic rates shown in bold. Rate sets are configured on the Advanced menu’s Radio Settings page. (See “Radio” on page 129.) The rates shown for an access point will always be the rates currently specified for that access point in its radio settings.

Advanced

Advanced Settings include the following:

- “Ethernet (Wired) Settings” on page 89
- “Wireless Settings” on page 97
- “Security” on page 101
- “Guest Login” on page 121
- “Virtual Wireless Networks” on page 125
- “Radio” on page 129
- “MAC Filtering” on page 135
- “Load Balancing” on page 139
- “Quality of Service” on page 143
- “Wireless Distribution System” on page 153
- “Time Protocol” on page 161
- “SNMP” on page 165
- “Reboot” on page 171
- “Reset Configuration” on page 171
- “Upgrade” on page 172
- “Backup/Restore” on page 174

Ethernet (Wired) Settings

Ethernet (Wired) Settings describe the configuration of your Ethernet local area network (LAN).

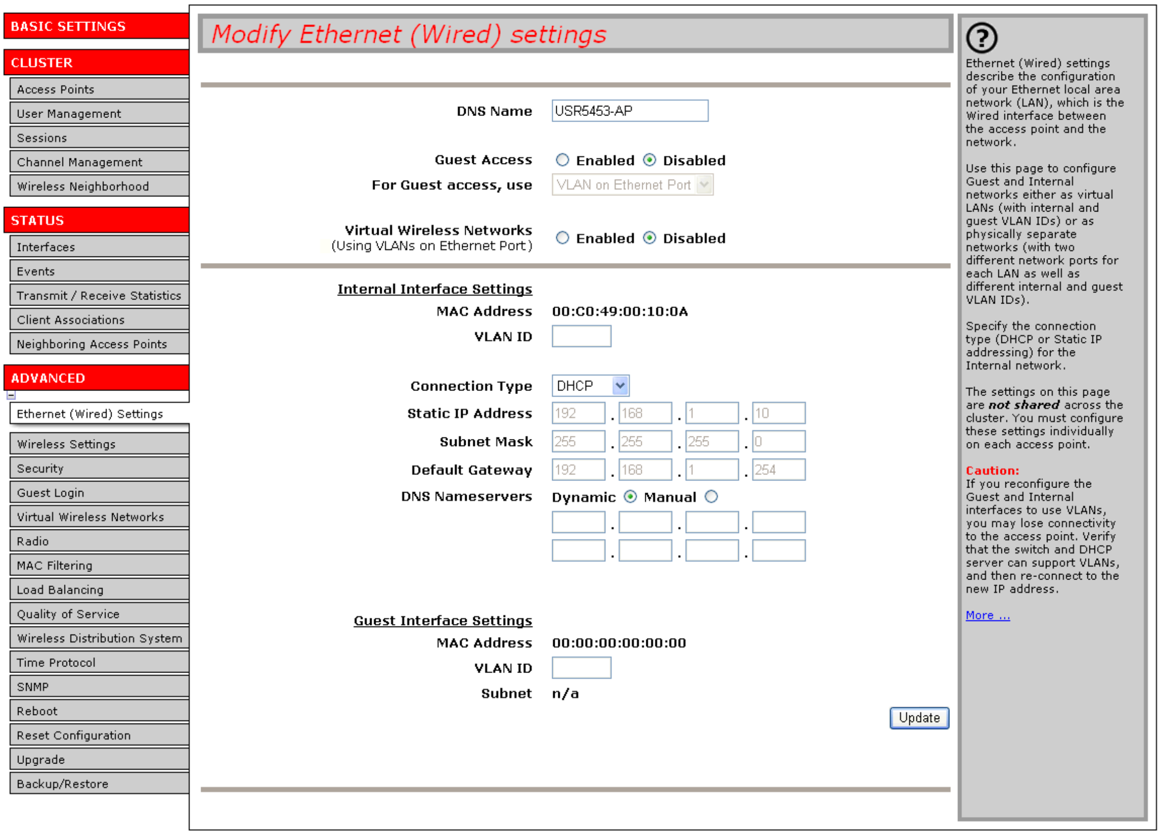
Note The Ethernet settings, including guest access, are not shared across the cluster. These settings must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click its IP Address link on the Cluster menu’s Access Points page of the current access point. For more information about which settings are shared by the cluster and which are not, see “Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?” on page 45.

The following sections describe how to configure the wired address and related settings on the Professional Access Point:

- Navigating to Ethernet (Wired) Settings
- Setting the DNS Name
- Managing Guest Access
    - Configuring an Internal LAN and a Guest Network
    - Enabling and Disabling Guest Access
    - Specifying a Virtual Guest Network
- Enabling and Disabling Virtual Wireless Networks on the Access Point
- Configuring Internal Interface Ethernet Settings
- Configuring Guest Interface Ethernet (Wired) Settings
- Updating Settings

Navigating to Ethernet (Wired) Settings

To set the wired address for an access point, click the Advanced menu's **Ethernet (Wired) Settings** tab, and update the fields as described below.



Modify Ethernet (Wired) settings

DNS Name	USR5453-AP
Guest Access	○ Enabled ● Disabled
For Guest access, use	VLAN on Ethernet Port
Virtual Wireless Networks (Using VLANs on Ethernet Port)	○ Enabled ● Disabled
Internal Interface Settings	
MAC Address	00:C0:49:00:10:0A
VLAN ID	
Connection Type	DHCP
Static IP Address	192 . 168 . 1 . 10
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 1 . 254
DNS Nameservers	Dynamic ● Manual ○
Guest Interface Settings	
MAC Address	00:00:00:00:00:00
VLAN ID	
Subnet	n/a

Ethernet (Wired) settings describe the configuration of your Ethernet local area network (LAN), which is the Wired interface between the access point and the network.

Use this page to configure Guest and Internal networks either as virtual LANs (with internal and guest VLAN IDs) or as physically separate networks (with two different network ports for each LAN as well as different internal and guest VLAN IDs).

Specify the connection type (DHCP or Static IP addressing) for the Internal network.

The settings on this page are ***not shared*** across the cluster. You must configure these settings individually on each access point.

Caution:
If you reconfigure the Guest and Internal interfaces to use VLANs, you may lose connectivity to the access point. Verify that the switch and DHCP server can support VLANs, and then re-connect to the new IP address.

More ...

Setting the DNS Name

Field	Description
DNS Name	Enter the DNS name for the access point in the text box. This is the host name. It may be provided by your ISP or network administrator, or you can provide your own. The rules for system names are: • This name can be up to 20 characters long. • Only letters, numbers, and dashes are allowed. • The name must start with a letter and end with either a letter or a number.

Managing Guest Access

You can provide controlled guest access over an isolated network and a secure internal LAN on the same Professional Access Point by using VLANs. You can also configure an access point for guest access only, without maintaining a separate secure LAN. The Guest settings on the **Ethernet (Wired) Settings** tab are required only if you want to use VLANs. For information about configuring an access point for guest access only, see “Configuring Guest Access without Virtual LANs” on page 124.

Configuring an Internal LAN and a Guest Network

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, one floor of a building. A LAN connects multiple computers and other network devices like storage and printers.

Ethernet is the most common technology for implementing a LAN. Wi-Fi (IEEE) is another very popular LAN technology.

The Professional Access Point allows you to configure two different LANs on the same access point: one for a secure *internal* LAN and another for a public *guest* network with no security and little or no access to internal resources. To configure these networks, you need to provide both wireless and Ethernet (wired) settings.

Information on how to configure the Ethernet (wired) settings is provided in the sections below.

(For information on how to configure the wireless settings, see “Wireless Settings” on page 97. For an overview of how to set up the Guest interface, see “Guest Login” on page 121.)

Enabling and Disabling Guest Access

The Professional Access Point ships with the Guest Access feature disabled by default. If you want to provide guest access while also maintaining a secure, internal network on your access point, enable **Guest**

Access on the Ethernet (Wired) Settings tab.

Field	Description
Guest Access	By default, the Professional Access Point ships with Guest Access disabled. • To enable Guest Access, click **Enabled**. • To disable Guest Access, click **Disabled**.

Specifying a Virtual Guest Network

If you enable Guest Access, you must represent both an Internal and a Guest Network on this access point virtually, by connecting the LAN port on the access point to a tagged port on a VLAN-capable switch and then defining two different virtual LANs on the Ethernet (Wired) Settings page. (For more information, see "Guest Login" on page 121.)

Choose virtually separate internal and guest LANs as described below.

Field	Description
Guest Access	• Select **Enabled** to enable Guest Access. (If you choose this option, you must select VLANs on the next setting **For Guest access, use**, and then provide details on VLAN or wired setting for the Guest Network on the rest of the page.) • Select **Disabled** to disable Guest Access
For Guest access, use	Specify a virtually separate guest network on this access point: • Choose **VLAN on Ethernet Port**. This will enable the VLAN settings where you must provide a VLAN ID. See also "Configuring Guest Interface Ethernet (Wired) Settings" on page 95. **Caution:** If you reconfigure the Guest and Internal interfaces to use VLANs, you may lose connectivity to the access point. First, be sure to verify that the switch and DHCP server you are using can support VLANs per the IEEE 802.1Q standard. After configuring the VLAN on the Advanced menu's Ethernet (Wired) Settings page, physically reconnect the Ethernet cable on the switch to the tagged packet (VLAN) port. Then, reconnect via the Web User Interface to the new IP address. (If necessary, check with the infrastructure support administrator regarding the VLAN and DHCP configurations.)

Enabling and Disabling Virtual Wireless Networks on the Access Point

If you want to configure the Internal network as a VLAN (whether or not you have a Guest network configured), you can enable **Virtual Wireless Networks** on the access point.

You must enable this feature if you want to configure additional virtual networks on VLANs on the Advanced menu's Virtual Wireless Networks page as described in "Virtual Wireless Networks" on page 125.

Field	Description
Virtual Wireless Networks (Using VLANs on Ethernet Port)	• Select **Enabled** to enable VLANs for the Internal network and for additional networks. If you choose this option, you can run the Internal network on a VLAN whether or not you have Guest Access configured and you can set up additional networks on VLANs using the Advanced menu's Virtual Wireless Networks page as described in "Virtual Wireless Networks" on page 125. • Select **Disabled** to disable the VLAN for the Internal network, and for any additional virtual networks on this access point.

Configuring Internal Interface Ethernet Settings

To configure Ethernet (Wired) settings for the Internal LAN, fill in the fields as described below.

Field	Description
MAC Address	Shows the MAC address for the Internal network interface for the LAN port on this access point. This is a read-only field.
VLAN ID	If you choose to configure Internal and Guest networks by VLANs, this field is enabled. Provide a number between 1 and 4094 for the Internal VLAN. This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE 802.1Q frames. The access point must be able to reach the DHCP server.

Field	Description
Connection Type	You can select **DHCP** or **Static IP**. The *Dynamic Host Configuration Protocol* (DHCP) is a protocol that specifies how a centralized server can provide network configuration information to devices on the network. A DHCP server offers a lease to the client. The information supplied includes the IP addresses and netmask plus the address of its DNS servers and gateway. Static IP indicates that all network settings are provided manually. You must provide the IP address for the Professional Access Point, its subnet mask, the IP address of the default gateway, and the IP address of at least one DNS name server. If you select **DHCP**, the Professional Access Point will acquire its IP Address, subnet mask, and DNS and gateway information from the DHCP Servers. If you select **Static IP**, fill in the **Static IP Address**, **Subnet Mask**, and **Default Gateway** fields. **Caution:** If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the connection type from DHCP to static IP. When you change the connection type to static IP, you can either assign a new Static IP Address to the access point or continue using the default address. USRobotics recommends assigning a new address so that if later you bring up another Professional Access Point on the same network, the IP addresses for the two APs will be unique. If you need to recover the default static IP address, you can do so by resetting the access point to the factory defaults as described in “Reset Configuration” on page 171.
Static IP Address	Enter the static IP address in the text boxes. This field is enabled only if you selected Static IP as the connection type.
Subnet Mask	Enter the **Subnet Mask** in the text boxes. You must obtain this information from your ISP or network administrator. This field is enabled only if you selected Static IP as the connection type.
Default Gateway	Enter the **Default Gateway** in the text boxes. This field is enabled only if you selected Static IP as the connection type.
DNS Nameservers	The *Domain Name Service* (DNS) is a system that resolves the descriptive name (*domainname*) of a network resource (for example, `www.usr.com`) to its numeric IP address (for example, `66.93.138.219`). A DNS server is called a *Nameserver*. There are usually two Nameservers; a Primary Nameserver and a Secondary Nameserver. You can choose **Dynamic** or **Manual** mode. • If you choose **Manual**, assign static IP addresses for the DNS servers manually. • If you choose **Dynamic**, the IP addresses for the DNS servers will be assigned automatically via DHCP. This option is only available if you specified **DHCP** for the **Connection Type**.

Configuring Guest Interface Ethernet (Wired) Settings

To configure Ethernet (Wired) Settings for the Guest interface, fill in the fields as described below.

Field	Description
MAC Address	Shows the MAC address for the Guest interface for the LAN port on this access point. This is a read-only field.
VLAN ID	If you choose to configure Internal and Guest networks by VLANs, this field will be enabled. Provide a number between 1 and 4094 for the Guest VLAN. Be sure to assign a different VLAN ID than the one used for the Internal network.
Subnet	Shows the subnetwork address for the Guest interface. For example, 192.168.1.0.

Updating Settings

To apply your changes, click **Update**.

Wireless Settings

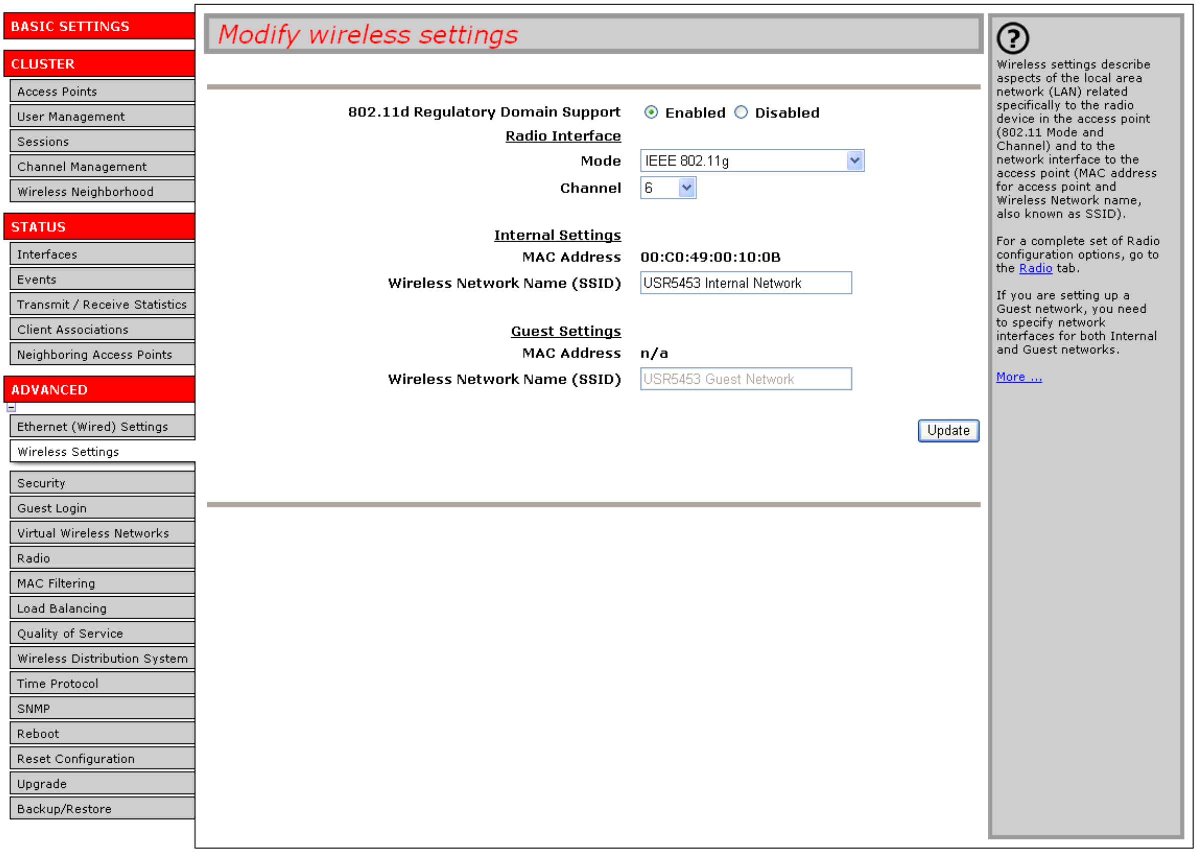
Wireless settings describe aspects of the local area network (LAN) related specifically to the radio device in the access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access point and wireless network name, also known as *SSID*).

The following sections describe how to configure the wireless address and related settings on the Professional Access Point:

- Navigating to Wireless Settings
- Configuring 802.11d Regulatory Domain Support
- Configuring the Radio Interface
- Configuring Internal LAN Wireless Settings
- Configuring Guest Network Wireless Settings
- Updating Settings

Navigating to Wireless Settings

To set the wireless address for an access point, click the Advanced menu's **Wireless Settings** tab, and update the fields as described below.



Modify wireless settings

802.11d Regulatory Domain Support ● Enabled ○ Disabled

Radio Interface

Mode: IEEE 802.11g

Channel: 6

Internal Settings

MAC Address: 00:C0:49:00:10:0B

Wireless Network Name (SSID): USR5453 Internal Network

Guest Settings

MAC Address: n/a

Wireless Network Name (SSID): USR5453 Guest Network

Wireless settings describe aspects of the local area network (LAN) related specifically to the radio device in the access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access point and Wireless Network name, also known as SSID).

For a complete set of Radio configuration options, go to the Radio tab.

If you are setting up a Guest network, you need to specify network interfaces for both Internal and Guest networks.

Configuring 802.11d Regulatory Domain Support

You can enable or disable IEEE 802.11d Regulatory Domain Support to broadcast the access point country code information as described below.

Field	Description
802.11d Regulatory Domain Support	Enabling support for IEEE 802.11d on the access point causes the access point to broadcast which country it is operating in as a part of its beacons: • To enable 802.11d regulatory domain support click **Enabled**. • To disable 802.11d regulatory domain support click **Disabled**. **Note:** IEEE 802.11d defines standard rules for the operation of IEEE 802.11 wireless LANs in any country without reconfiguration. IEEE 802.11d allows client devices to operate in any country without reconfiguration.

Configuring the Radio Interface

The radio interface allows you to set the radio Channel and 802.11 mode as described below.

Field	Description
Mode	The *Mode* defines the *Physical Layer* (PHY) standard being used by the radio. Select one of these modes: • IEEE 802.11b • IEEE 802.11g
Channel	Select the **Channel**. The range of channels is 1 through 11. The Channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R). The default is **Auto**, which picks the least busy channel at startup time.

Configuring Internal LAN Wireless Settings

The **Internal Settings** describe the MAC Address and Network Name (also known as the SSID) for the internal *Wireless LAN* (WLAN) as described below.

Field	Description
MAC Address	Shows the MAC address for the Internal interface for this access point. This is a read-only field that you cannot change. Although this access point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. This is accomplished by using multiple *Basic Service Set Identifiers* (BSSIDs) for a single access point. The MAC address shown for the Internal access point is the BSSID for the Internal interface.
Wireless Network Name (SSID)	Enter the SSID for the internal WLAN. The *Service Set Identifier* (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Configuring Guest Network Wireless Settings

The **Guest Settings** describe the MAC Address (read-only) and wireless network name (SSID) for the *Guest Network* as described below. Configuring an access point with two different network names (SSIDs) allows you to implement the Guest interface feature on the Professional Access Point. For more information, see “Guest Login” on page 121.

Field	Description
MAC Address	Shows the MAC address for the Guest interface for this access point. This is a read-only field. Although this access is point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. This is accomplished by using multiple *Basic Service Set Identifiers* (BSSID) for a single access point. The MAC address shown for the Guest access point is the BSSID for the Guest interface.
Wireless Network Name (SSID)	Enter the SSID for the guest network. The *Service Set Identifier* (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID. For the guest network, provide an SSID that is different from the internal SSID and easily identifiable as the guest network. If you are configuring an access point for guest access only, without also maintaining a separate, secure network, you do not need to specify a Guest network SSID. You will have only one network: the Internal network.

Updating Settings

To apply your changes, click **Update**.

Security

The following sections describe how to configure security settings on the Professional Access Point:

- Understanding Security Issues on Wireless Networks
  - How Do I Know Which Security Mode to Use?
  - Comparison of Security Modes for Key Management, Authentication and Encryption Algorithms
  - Does Prohibiting the Broadcast of SSID Enhance Security?
  - How Does Station Isolation Protect the Network?
- Navigating to Security Settings
- Configuring Security Settings
  - Broadcast SSID, Station Isolation, and Security Mode
  - None
  - Static WEP
  - IEEE 802.1x
  - WPA/WPA2 Personal (PSK)
  - WPA/WPA2 Enterprise (RADIUS)
- Updating Settings

Understanding Security Issues on Wireless Networks

Wireless mediums are inherently less secure than wired mediums. For example, an Ethernet NIC transmits its packets over a physical medium such as coaxial cable or twisted pair. A wireless NIC broadcasts radio signals over the air allowing a wireless LAN to be easily tapped without physical access or sophisticated equipment. A hacker equipped with a laptop, a wireless NIC, and a bit of knowledge can easily attempt to compromise your wireless network. By using a sophisticated antenna on the client, a hacker may even be able to connect to the network from many miles away.

The Professional Access Point provides a number of authentication and encryption schemes to ensure that your wireless infrastructure is accessed only by the intended users. The details of each security mode are described in the sections below.

How Do I Know Which Security Mode to Use?

In general, USRobotics recommends that on your Internal network you use the most robust security mode that is feasible in your environment. When configuring security on the access point, you first must choose the security mode. Then, in some modes you must choose an authentication algorithm and whether to allow clients not using the specified security mode to associate.

Wi-Fi Protected Access (WPA) with *Remote Authentication Dial-In User Service* (RADIUS) using the CCMP (AES) encryption algorithm provides the best data protection available and is clearly the best choice if all client devices are equipped with WPA supplicants. However, backward compatibility or interoperability issues with clients or even with other access points may require that you configure WPA with RADIUS with a different encryption algorithm or choose one of the other security modes.

However, security may not be as much of a priority on some types of networks. If you are simply providing internet and printer access, **None** may be the appropriate choice. To prevent clients from accidentally discovering and connecting to your network, you can disable the broadcast SSID so that your network name is not advertised. If the network is sufficiently isolated from access to sensitive information, this may offer enough protection in some situations.

Following is a brief discussion of the factors that make one mode more secure than another, a description of each mode offered, and when to use each mode.

Comparison of Security Modes for Key Management, Authentication and Encryption Algorithms

The major factors that determine the effectiveness of a security protocol are:

- How the protocol manages keys
- Presence or absence of integrated user authentication in the protocol
- Encryption algorithm or formula the protocol uses to encode and decode the data

Following is a list of the security modes available on the Professional Access Point along with a description of the key management, authentication, and encryption algorithms used in each mode. Each discussion includes suggestions as to when one mode might be more appropriate than another.

- When to Use No Security
- When to Use Static WEP
- When to Use IEEE 802.1x
- When to Use WPA/WPA2 Personal (PSK)
- When to Use WPA/WPA2 Enterprise (RADIUS)

When to Use No Security

None is a security mode option. In this mode, the data is not encrypted. Instead, the data is sent as plain text across the network. No key management, data encryption, or user authentication is used.

RECOMMENDATIONS

None is not recommended for regular use on the Internal network because the Internal network should have some level of security. Use **None** on the Internal network for initial setup, testing, or problem solving only.

SEE ALSO

For information on how to configure this mode, see “None” on page 108 under “Configuring Security Settings”.

When to Use Static WEP

Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

Key Management	Encryption Algorithm	User Authentication
Static WEP uses a fixed key that is provided by the administrator. WEP keys are indexed in different slots (up to four on the Professional Access Point). The client devices must have the same key indexed in the same slot to access data on the access point.	An RC4 stream cipher is used to encrypt the frame body and *cyclic redundancy checking* (CRC) of each 802.11 frame.	If you set the **Authentication Algorithm** to **Shared Key**, this protocol provides a rudimentary form of user authentication. However, if the **Authentication Algorithm** is set to **Open System**, no authentication is performed. If the algorithm is set to **Both**, only WEP clients are authenticated.

RECOMMENDATIONS

Static WEP was designed to provide security equivalent of sending unencrypted data through an Ethernet connection, however it has major flaws and it does not provide even this intended level of security.

Therefore, Static WEP is not recommended as a secure mode. The only time to use Static WEP is when interoperability issues make it the only option available to you and you are not concerned with the potential of exposing the data on your network.

SEE ALSO

For information on how to configure Static WEP security mode, see “Static WEP” on page 108 under “Configuring Security Settings”.

When to Use IEEE 802.1x

IEEE 802.1x is the standard for passing the Extensible Authentication Protocol (EAP) over an 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). This is a newer, more secure standard than Static WEP.

Key Management	Encryption Algorithm	User Authentication
IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station.	An RC4 stream cipher is used to encrypt the frame body and *cyclic redundancy checking* (CRC) of each 802.11 frame.	IEEE 802.1x mode supports a variety of authentication methods, like certificates, Kerberos, and public key authentication with a RADIUS server. You have a choice of using the Professional Access Point embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

Recommendations

IEEE 802.1x mode is a better choice than Static WEP because keys are dynamically generated and changed periodically. However, the encryption algorithm used is the same as that of Static WEP and is therefore not as reliable as the more advanced encryption methods such as TKIP and CCMP (AES) used in *Wi-Fi Protected Access* (WPA) or WPA2.

Additionally, compatibility issues may be cumbersome because of the variety of authentication methods supported and the lack of a standard implementation method.

Therefore, IEEE 802.1x mode is not as secure a solution as *Wi-Fi Protected Access* (WPA) or WPA2.

See Also

For information on how to configure IEEE 802.1x security mode, see “IEEE 802.1x” on page 114 under “Configuring Security Settings”.

When to Use WPA/WPA2 Personal (PSK)

Wi-Fi Protected Access 2 (WPA2) Personal *Pre-Shared Key* (PSK) is an implementation of the Wi-Fi Alliance IEEE 802.11i standard, which includes *Advanced Encryption Algorithm* (AES), *Counter mode/ CBC-MAC Protocol* (CCMP), and *Temporal Key Integrity Protocol* (TKIP) mechanisms. This mode offers the same encryption algorithms as WPA 2 with RADIUS but without the ability to integrate a RADIUS server for user authentication.

This security mode is backward compatible for wireless clients that support only the original WPA.

Key Management	Encryption Algorithms	User Authentication
WPA/WPA2 Personal (PSK) provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station.	• *Temporal Key Integrity Protocol* (TKIP) • *Counter mode/CBC-MAC Protocol* (CCMP) *Advanced Encryption Standard* (AES)	The use of a Pre-Shared (PSK) key provides user authentication similar to that of shared keys in WEP.

RECOMMENDATIONS

WPA/WPA2 Personal (PSK) is not recommended for use with the Professional Access Point when WPA/ WPA2 Enterprise (RADIUS) is an option.

USRobotics recommends that you use WPA/WPA2 Enterprise (RADIUS) mode instead, unless you have interoperability issues that prevent you from using this mode.

For example, some devices on your network may not support WPA or WPA2 with EAP talking to a RADIUS server. Embedded printer servers or other small client devices with very limited space for implementation may not support RADIUS. For such cases, USRobotics recommends that you use WPA/ WPA2 Personal (PSK).

SEE ALSO

For information on how to configure this security mode, see “WPA/WPA2 Personal (PSK)” on page 115.

When to Use WPA/WPA2 Enterprise (RADIUS)

Wi-Fi Protected Access 2 (WPA2) with *Remote Authentication Dial-In User Service* (RADIUS) is an implementation of the Wi-Fi Alliance IEEE 802.11i standard, which includes *Advanced Encryption Standard* (AES), *Counter mode/CBC-MAC Protocol* (CCMP), and *Temporal Key Integrity Protocol* (TKIP) mechanisms. This mode requires the use of a RADIUS server to authenticate users. WPA/WPA2 Enterprise (RADIUS) provides the best security available for wireless networks.

This security mode also provides backward compatibility for wireless clients that support only the original WPA.

Key Management	Encryption Algorithms	User Authentication
WPA/WPA2 Enterprise (RADIUS) mode provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station.	• *Temporal Key Integrity Protocol* (TKIP) • *Counter mode/CBC-MAC Protocol* (CCMP) *Advanced Encryption Standard* (AES)	*Remote Authentication Dial-In User Service* (RADIUS) You have a choice of using the Professional Access Point embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

RECOMMENDATIONS

WPA/WPA2 Enterprise (RADIUS) mode is the **recommended mode**. The CCMP (AES) and TKIP encryption algorithms used with WPA modes are far superior to the RC4 algorithm used for Static WEP or IEEE 802.1x modes. Therefore, CCMP (AES) or TKIP should be used whenever possible. All WPA modes allow you to use these encryption schemes, so WPA security modes are recommended above the others when using WPA is an option.

Additionally, this mode incorporates a RADIUS server for user authentication, which gives it an edge over WPA/WPA2 Personal (PSK) mode.

Use the following guidelines for choosing options within the WPA/WPA2 Enterprise (RADIUS) mode security mode:

1. The best security you can have to-date on a wireless network is WPA/WPA2 Enterprise (RADIUS) mode using CCMP (AES) encryption algorithm. AES is a symmetric 128-bit block data encryption technique that works on multiple layers of the network. It is the most effective encryption system currently available for wireless networks. If all clients or other APs on the network are WPA/CCMP compatible, use this encryption algorithm. If all clients are WPA2 compatible, choose to support only WPA2 clients.

2. The second best choice is WPA/WPA2 Enterprise (RADIUS) with the encryption algorithm set to **Both** (that is, both TKIP and CCMP). This lets WPA clients without CCMP associate, uses TKIP for encrypting Multicast and Broadcast frames, and allows clients to select whether to use CCMP or TKIP for Unicast (access-point-to-single-station) frames. This WPA configuration allows more interoperability, at the expense of some security. Clients that support CCMP can use it for their Unicast frames. If you encounter access-point-to-station interoperability problems with the **Both** encryption algorithm setting, then you will need to select TKIP instead.

3. The third best choice is WPA/WPA2 Enterprise (RADIUS) with the encryption algorithm set to TKIP. Some clients have interoperability issues with CCMP and TKIP enabled at same time. If you encounter this problem, then choose TKIP as the encryption algorithm. This is the standard WPA mode, and most interoperable mode with client wireless software security features. TKIP is the only encryption algorithm that is being tested in Wi-Fi WPA certification.

SEE ALSO

For information on how to configure this security mode, see “WPA/WPA2 Enterprise (RADIUS)” on page 117 under “Configuring Security Settings”.

Does Prohibiting the Broadcast of SSID Enhance Security?

You can prohibit the broadcast of the AP’s SSID to discourage stations from automatically discovering your access point. When the access point’s SSID broadcast is prohibited, the network name is not displayed in the **List of Available Networks** on a client device. Instead, the client must have the exact network name configured in the supplicant before the client will be able to connect.

Prohibiting the SSID broadcast is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect or to monitor insecure traffic.

This offers a minimum level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.

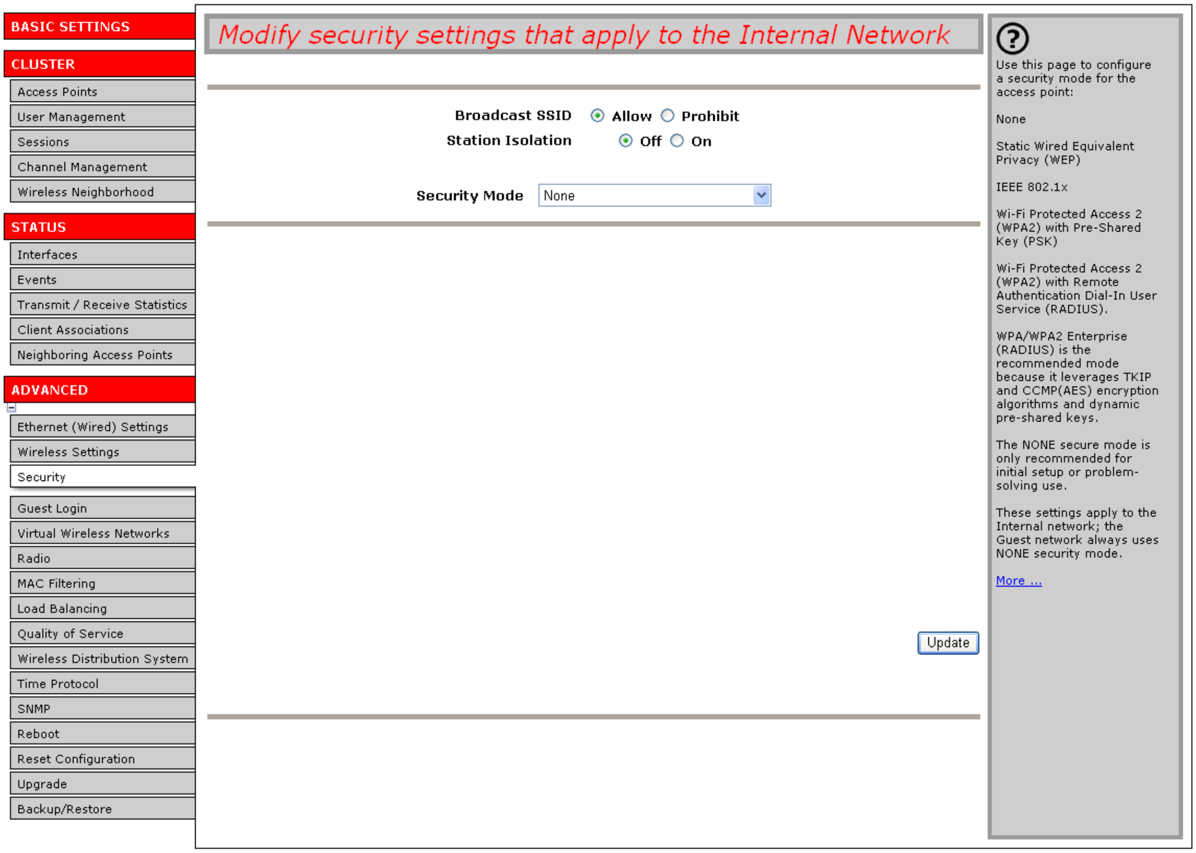
How Does Station Isolation Protect the Network?

When **Station Isolation** is enabled, the access point blocks communication between wireless clients. The access point allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients.

The traffic blocking extends to wireless clients connected to the network via WDS links; these clients cannot communicate with each other when Station Isolation is on. See “Wireless Distribution System” on page 153 for more information about WDS.

Navigating to Security Settings

To set the security mode, click the Advanced menu's **Security** tab, and update the fields as described below.



Modify security settings that apply to the Internal Network

Broadcast SSID ● Allow ○ Prohibit

Station Isolation ● Off ○ On

Security Mode: None

Use this page to configure a security mode for the access point:

None

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access 2 (WPA2) with Pre-Shared Key (PSK)

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS).

WPA/WPA2 Enterprise (RADIUS) is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The NONE secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses NONE security mode.

Configuring Security Settings

The following configuration information explains how to configure security modes on the access point. Keep in mind that each wireless client that wants to exchange data with the access point must be configured with the same security mode and encryption key settings consistent with access point security.

Broadcast SSID, Station Isolation, and Security Mode

To configure security on the access point, select a security mode and fill in the related fields as described in the following table. You can also allow or prohibit the Broadcast SSID and enable or disable Station

Isolation as extra precautions as mentioned below.

Field	Description
Broadcast SSID	Select the **Broadcast SSID** setting by clicking **Allow** or **Prohibit**. By default, the access point broadcasts the *Service Set Identifier* (SSID) in its beacon frames. You can prohibit this broadcast to discourage stations from automatically discovering your access point. When the access point's broadcast SSID is suppressed, the network name will not be displayed in the **List of Available Networks** on a client device. Instead, the client must have the exact network name configured in the supplicant before the client will be able to connect. You can use the Command Line Interface to prohibit the broadcast of the SSID on the Guest Network. For the command syntax, see "Set the Broadcast SSID (Allow or Prohibit)" on page 215.
Station Isolation	Select **Off** to disable station isolation or **On** to enable it. • When station isolation is **Off**, wireless clients can communicate with one another normally by sending traffic through the access point. • When station isolation is **On**, the access point blocks communication between wireless clients. The access point allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients. The traffic blocking extends to wireless clients connected to the network via WDS links; these clients cannot communicate with each other when station isolation is on. See "Wireless Distribution System" on page 153 for more information about WDS.
Security Mode	Select the **Security Mode**. Select one of the following: • **None** • **Static WEP** • **IEEE 802.1x** • **WPA/WPA2 Personal (PSK)** • **WPA/WPA2 Enterprise (RADIUS)**

None

None means that any data transferred to and from the Professional Access Point is not encrypted.

There are no further options for this mode.Running without security can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the Internal network because it is not secure.

Static WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

You cannot mix 64-bit and 128-bit WEP keys between the access point and its clients.

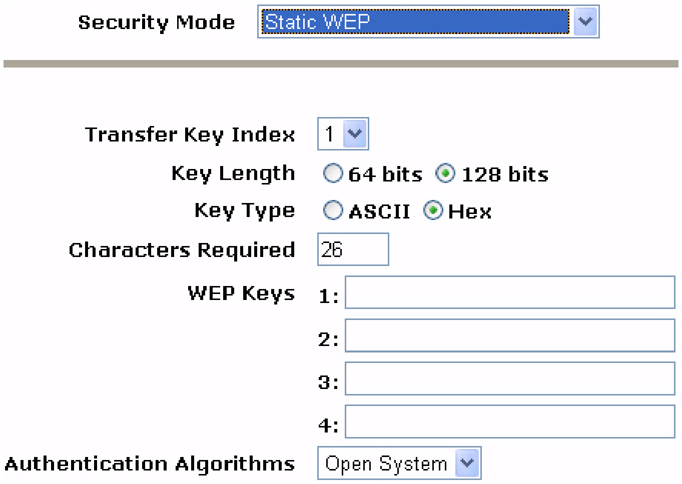
Static WEP is not the most secure mode available, but it offers more protection than **None** as it does prevent an outsider from easily sniffing out unencrypted wireless traffic. (For more secure modes, see the sections on “IEEE 802.1x” on page 114, “WPA/WPA2 Enterprise (RADIUS)” on page 117, or “WPA/WPA2 Personal (PSK)” on page 115.)

WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a stream cipher called *RC4*.)

The access point uses a key to transmit data to the clients. Each client must use that same key to decrypt data it receives from the access point.

Clients can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

If you selected **Static WEP** as the security mode, provide the following on the access point settings:



Security Mode	Static WEP
Transfer Key Index	1
Key Length	○ 64 bits ● 128 bits
Key Type	○ ASCII ● Hex
Characters Required	26
WEP Keys	1:
	2:
	3:
	4:
Authentication Algorithms	Open System

.

Field	Description
Transfer Key Index	Select a key index. Key indexes 1 through 4 are available. The default is 1. The transfer key index indicates which WEP key the access point will use to encrypt the data it transmits.
Key Length	Specify one of the following lengths for the key: • **64 bits** • **128 bits**
Key Type	Select one of the following key types: • **ASCII** • **Hex**
Characters Required	Indicates the number of characters required in the WEP key. The number is updated automatically based on how you set **Key Length** and **Key Type**.
WEP Keys	You can specify up to four WEP keys. In each text box, enter a string of characters for one key. If you selected **ASCII**, enter any combination of integers and letters `0-9, a-z`, and `A-Z`. If you selected **HEX**, enter hexadecimal digits (any combination of `0-9` and `a-f` or `A-F`). Use the same number of characters for each key as specified in the **Characters Required** field. These are the RC4 WEP keys shared with the stations using the access point. Each client must be configured to use one of these same WEP keys in the same slot as specified here on the access point. (See “Rules to Remember for Static WEP” on page 111.)

Field	Description
Authentication Algorithm	The authentication algorithm defines the method used to determine whether a client is allowed to associate with an access point when static WEP is the security mode. Specify the authentication algorithm you want to use by choosing one of the following: • **Open System** • **Shared Key** • **Both** **Open System** authentication allows any client to associate with the access point whether that client has the correct WEP key or not. This algorithm is also used in None, IEEE 802.1x, and WPA modes. When the authentication algorithm is set to **Open System**, any client can associate with the access point. That a client is allowed to *associate* does not ensure that the client can exchange traffic with an access point. A client must have the correct WEP key to be able to successfully access and decrypt data from an access point, and to transmit readable data to the access point. **Shared Key** authentication requires the client to have the correct WEP key in order to associate with the access point. When the authentication algorithm is set to **Shared Key**, a station with an incorrect WEP key will not be able to associate with the access point. **Both** is the default. When the authentication algorithm is set to **Both**: • Clients configured to use WEP in shared key mode must have a valid WEP key in order to associate with the access point. • Clients configured to use WEP in an open system mode (shared key mode not enabled) will be able to associate with the access point even if they do not have the correct WEP key.

Rules to Remember for Static WEP

- All clients must have the Wireless LAN (WLAN) security set to WEP, and all clients must have one of the WEP keys specified on the access point in order to decode access-point-to-station data transmissions.

- The access point must have all keys used by clients for station-to-access-point transmit so that it can decode the station transmissions.

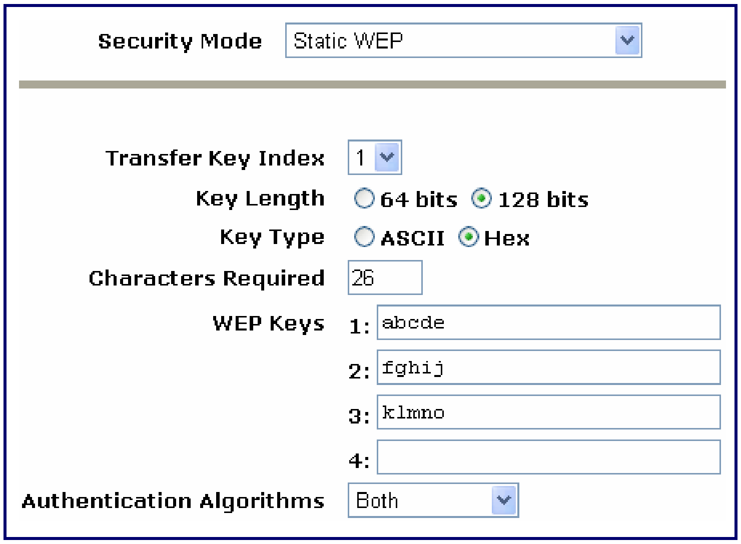
- The same key must occupy the same slot on all nodes (access point and clients). For example, if the access point defines `abc123` key as WEP key 3, then the clients must define that same string as WEP key 3.

- On some wireless client software (like Funk Odyssey), you can configure multiple WEP keys and define a client transfer key index, then set the stations to encrypt the data they transmit using different keys. This ensures that neighbouring APs cannot decode each other’s transmissions.

Example of Using Static WEP

For a simple example, suppose that you configure three WEP keys on the access point. In this example, the Transfer Key Index for the access point is set to 3. This means that the WEP key in slot 3 is the key that the access point will use to encrypt the data it sends.

Figure 7. Setting the Access Point Transfer Key on the Access Point.



Security Mode: Static WEP

Transfer Key Index: 1

Key Length: ○ 64 bits ● 128 bits

Key Type: ○ ASCII ● Hex

Characters Required: 26

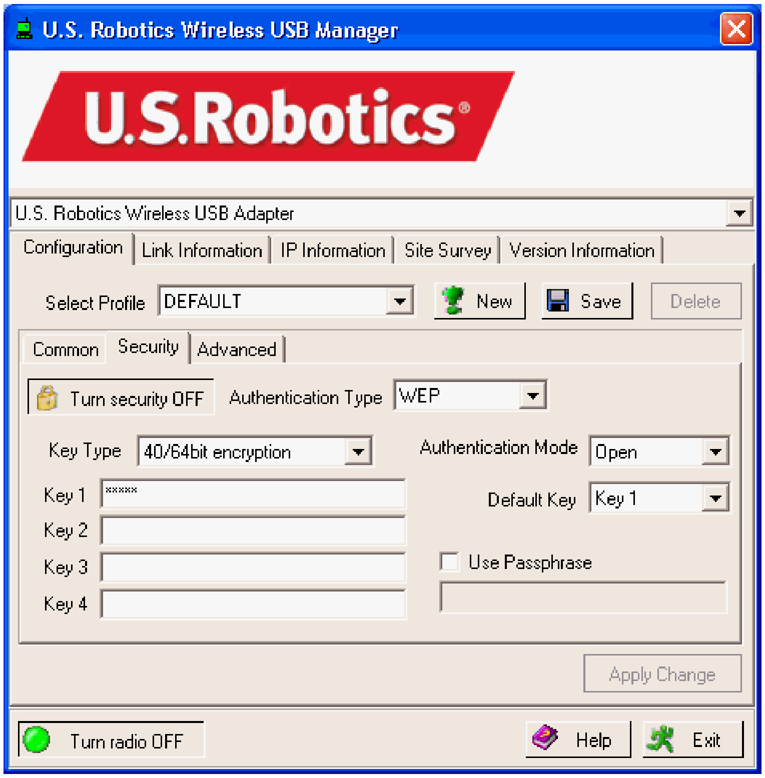
WEP Keys
1: abcde
2: fghij
3: klmno
4:

Authentication Algorithms: Both

You must then set all clients to use WEP and provide each client with one of the slot and key combinations you defined on the access point.

The following example will set WEP key 1 on a Windows client.

Figure 8. Providing a Wireless Client with a WEP Key



U.S. Robotics Wireless USB Adapter

Select Profile: DEFAULT

Authentication Type: WEP

Key Type: 40/64bit encryption

Authentication Mode: Open

Key 1: *****

Key 2:

Key 3:

Key 4:

Default Key: Key 1

□ Use Passphrase

If you have a second client, that client also needs to have one of the WEP keys defined on the access point. You could give it the same WEP key that you gave to the first station. Or, for a more secure solution, you could give the second station a different WEP key (key 2, for example) so that the two stations cannot decrypt each other's transmissions.

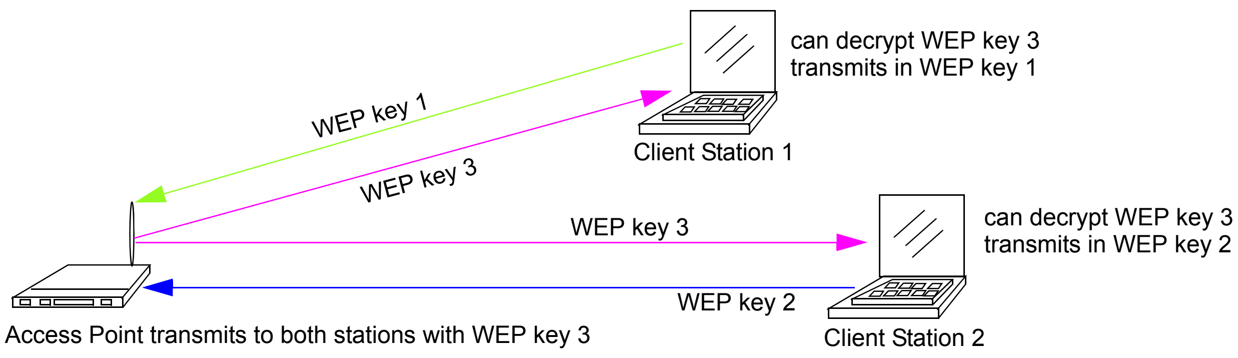
Static WEP with Transfer Key Indexes on Client Devices

Some Wireless client software, such as like Funk Odyssey, lets you configure multiple WEP keys and set a transfer index on the client; then you can specify different keys to be used for station-to-access-point transmissions. (The standard Windows wireless client software does not allow you to do this.)

To build on the previous example, using Funk Odyssey client software you could give each of the clients WEP key 3 so that they can decode the access point transmissions with that key and also give client 1 WEP key 1 and set this as the client 1's transfer key index. You could then give client 2 WEP key 2 and set this as client 2's transfer key index.

Figure 9 illustrates the dynamics of the access point and two clients using multiple WEP keys and a transfer key index.

Figure 9. Example of Using Multiple WEP Keys and Transfer Key Index on Client Devices



IEEE 802.1x

IEEE 802.1x is the standard that defines port-based authentication and provides a framework for implementing key management. Extensible Authentication Protocol (EAP) packets are sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

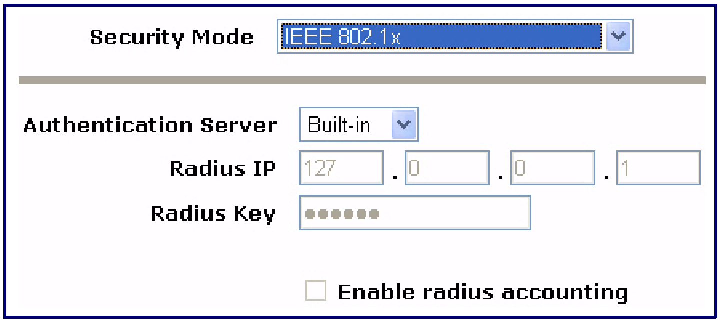
The IEEE 802.1x security mode requires the use of a RADIUS server to authenticate users and requires configuration of user accounts via the Cluster menu's User Management page.

The access point requires a RADIUS server capable of EAP, such as the Microsoft Internet Authentication Server or the Professional Access Point internal authentication server. To work with Windows clients, the authentication server must support Protected EAP (PEAP) and MSCHAP V2.

When configuring IEEE 802.1x mode, you can use either the embedded RADIUS server or an external RADIUS server that you provide. The Professional Access Point embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you use your own RADIUS server, you can use any of a variety of authentication methods that the IEEE 802.1x mode supports, including certificates, Kerberos, and public key authentication. Keep in mind, however, that the clients must be configured to use the same authentication method being used by the access point.

If you select **IEEE 802.1x** Security Mode, you must provide the following:



Security Mode: IEEE 802.1x

Authentication Server: Built-in

Radius IP: 127 . 0 . 0 . 1

Radius Key: ●●●●●●

☐ Enable radius accounting

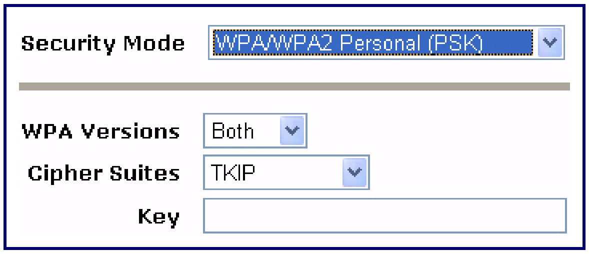
Field	Description
Authentication Server	Select one of the following: • **Built-in**—To use the authentication server provided with the Professional Access Point. If you choose this option, you do not have to provide the Radius IP and Radius Key; they are automatically provided. • **External**—To use an external authentication server. If you choose this option you must supply the Radius IP and Radius Key of the server you want to use. **Note:** The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides.The RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable on the Professional Access Point. (The access point is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)
Radius IP	Enter the Radius IP in the text box. The *Radius IP* is the IP address of the RADIUS server. The Professional Access Point internal authentication server is `127.0.0.1` For information on setting up user accounts, see “User Management” on page 53.
Radius Key	Enter the Radius Key in the text box. The *Radius Key* is the shared secret key for the RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type. (The Professional Access Point internal authentication server key is `secret`.) This value is never sent over the network.
Enable RADIUS Accounting	Click **Enable RADIUS Accounting** if you want to track and measure the resources that a particular user has consumed. Resources measured include system time, amount of data transmitted and received, and so on.

WPA/WPA2 Personal (PSK)

Wi-Fi Protected Access 2 (WPA2) with *Pre-Shared Key* (PSK) is a Wi-Fi Alliance IEEE 802.11i standard, which includes *Advanced Encryption Algorithm* (AES), *Counter mode/CBC-MAC Protocol* (CCMP), and *Temporal Key Integrity Protocol* (TKIP) mechanisms. The Personal version of WPA2 employs a pre-shared key (instead of using IEEE 802.1x and EAP as is used in the Enterprise WPA2 security mode). The PSK is used for an initial check of credentials only.

This security mode is backward-compatible for wireless clients that support the original WPA.

If you select **WPA/WPA2 Personal (PSK)** Security Mode, you must provide the following:



Security Mode	WPA/WPA2 Personal (PSK)
WPA Versions	Both
Cipher Suites	TKIP
Key	

Field	Description
WPA Versions	Select the types of clients you want to support: • **WPA**—If all clients on the network support the original WPA, but none support the newer WPA2, then select **WPA** • **WPA2**—If all clients on the network support WPA2, USRobotics suggests using **WPA2**, which provides the best security per the IEEE 802.11i standard. • **Both**—If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select **Both**. This option lets both WPA and WPA2 clients associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
Cipher Suites	Select the cipher you want to use from the list: • **TKIP**—TKIP *(Temporal Key Integrity Protocol*) is the default. TKIP provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be reused to encrypt data (a weakness of WEP). TKIP uses a 128-bit temporal key shared by clients and access points. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. • **CCMP (AES)**—*Counter mode/CBC-MAC Protocol* (CCMP) is an encryption method for IEEE 802.11i that uses the **Advanced Encryption Algorithm** (AES). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity. • **Both**—When the authentication algorithm is set to **Both**, both TKIP and AES clients can associate with the access point. WPA clients must have one of the following to be able to associate with the access point: • A valid TKIP key • A valid CCMP (AES) key Clients not configured to use a WPA-PSK will not be able to associate with the access point.

Field	Description
Key	The *Pre-shared Key* is the shared secret key for WPA-PSK. Enter a string of at least 8 characters to a maximum of 63 characters.

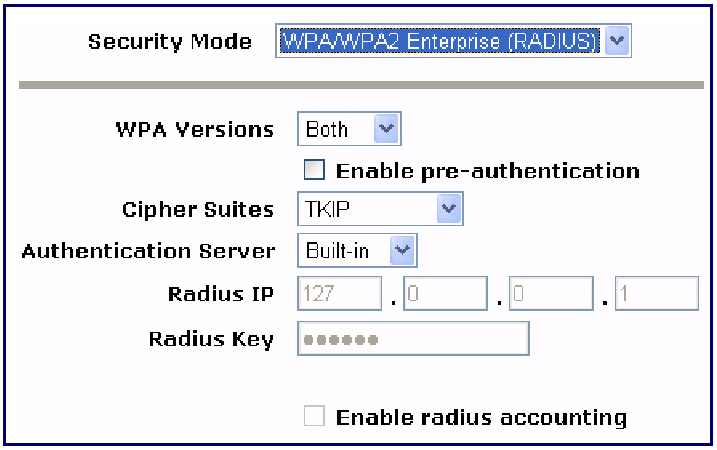
WPA/WPA2 Enterprise (RADIUS)

Wi-Fi Protected Access 2 (WPA2) with *Remote Authentication Dial-In User Service* (RADIUS) is an implementation of the Wi-Fi Alliance IEEE 802.11i standard, which includes *Advanced Encryption Standard* (AES), *Counter mode/CBC-MAC Protocol* (CCMP), and *Temporal Key Integrity Protocol* (TKIP) mechanisms. The Enterprise mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts via the Cluster menu's User Management page.

This security mode is backward-compatible with wireless clients that support the original WPA.

When configuring WPA2 Enterprise (RADIUS) mode, you can use either the built-in RADIUS server or an external RADIUS server that you provide. The Professional Access Point built-in RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you select **WPA/WPA2 Enterprise (RADIUS)** Security Mode, you must provide the following:



Security Mode	WPA/WPA2 Enterprise (RADIUS)
WPA Versions	Both
	☐ Enable pre-authentication
Cipher Suites	TKIP
Authentication Server	Built-in
Radius IP	127 . 0 . 0 . 1
Radius Key	••••••
	☐ Enable radius accounting

Field	Description
WPA Versions	Select the types of clients you want to support: • **WPA**—If all clients on the network support the original WPA, but none support the newer WPA2, then select **WPA** • **WPA2**—If all clients on the network support WPA2, USRobotics suggests using **WPA2**, which provides the best security per the IEEE 802.11i standard. • **Both**—If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select **Both**. This option lets both WPA and WPA2 clients associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.

Field	Description
Enable pre-authentication	If for **WPA Versions** you select **WPA2** or **Both**, you can enable pre-authentication for WPA2 clients. Click **Enable pre-authentication** if you want WPA2 wireless clients to send pre-authentication packet. The pre-authentication information will be relayed from the access point the client is currently using to the target access point. Enabling this feature can help speed up authentication for roaming clients who connect to multiple access points. This option does not apply if you selected **WPA** for WPA Versions because the original WPA does not support this feature.
Cipher Suites	Select the cipher you want to use from the list: • **TKIP—***Temporal Key Integrity Protocol* (TKIP) provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be reused to encrypt data (a weakness of WEP). TKIP uses a 128-bit temporal key shared by clients and access points. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. • **CCMP (AES)**—*Counter mode/CBC-MAC Protocol* (CCMP) is an encryption method for IEEE 802.11i that uses the **Advanced Encryption Algorithm** (AES). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity. • **Both**—The default. When the authentication algorithm is set to **Both**, both TKIP and AES clients can associate with the access point. Clients configured to use WPA with RADIUS must have one of the following to be able to associate with the access point: • A valid TKIP RADIUS IP address and RADIUS Key • A valid CCMP (AES) IP address and RADIUS Key Clients not configured to use WPA with RADIUS will not be able to associate with access point.
Authentication Server	Select one of the following from list: • **Built-in**—To use the authentication server provided with the Professional Access Point. If you choose this option, you do not have to provide the Radius IP and Radius Key; they are automatically provided. • **External**—To use an external authentication server. If you choose this option you must supply a Radius IP and Radius Key of the server you want to use. **Note:** The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the Professional Access Point, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable. The Professional Access Point is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.

Field	Description
Radius IP	Enter the Radius IP. The *Radius IP* is the IP address of the RADIUS server. (The Professional Access Point internal authentication server is `127.0.0.1`.) For information on setting up user accounts, see “User Management” on page 53.
Radius Key	Enter the Radius Key. The *Radius Key* is the shared secret key for the RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type. (The Professional Access Point internal authentication server key is `secret`.) This value is never sent over the network.
Enable RADIUS Accounting	Click **Enable RADIUS Accounting** if you want to enforce authentication for WPA clients with user names and passwords for each client. See also “User Management” on page 53.

Updating Settings

To apply your changes, click **Update**.

Guest Login

The Professional Access Point's Guest Interface features allow you to configure the access point for controlled guest access to an isolated network. You can configure the access point for guest access only, or you can configure it to broadcast and function as two different wireless networks: a secure Internal LAN and a public Guest network.

Guest clients can access the guest network without a user name or password. When guests log in, they see a guest Welcome screen (also known as a *captive portal*).

The following sections are included here:

- Configuring Guest Access Using Virtual LANs
  - Configuring a Guest Network on a Virtual LAN
  - Configuring the Welcome Screen (Captive Portal)
  - Using the Guest Network
- Configuring Guest Access without Virtual LANs
  - Configuring a Guest Network on a Dedicated Access Point
  - Using the Guest Network

Configuring Guest Access Using Virtual LANs

If you implement the guest interface with VLANs, you can define unique parameters for guest connectivity and isolate guest clients from other, more sensitive areas of the network. No security is provided on the guest network; only **None** is allowed as the security mode.

Simultaneously, you can configure a secure internal network (using the same access point as your guest interface) that provides full access to protected information behind a firewall and requires secure logins or certificates for access.

Note The VLAN implementation of the Guest Interface uses the *multiple BSSID* and *Virtual LAN* (VLAN) technologies that are built into the Professional Access Point. The Internal and Guest networks are implemented as multiple BSSIDs on the same access point, each with different network names (SSIDs) on the Wireless interface and different VLAN IDs on the Wired interface.

Configuring a Guest Network on a Virtual LAN

To configure the Guest interface on the Professional Access Point, perform these configuration steps:

1. To implement the Guest interface using VLANs, configure the access point to represent two virtually separate networks as described in “Configuring a Guest Network on a Virtual LAN” on page 121.

2. Set up the guest Welcome screen for the guest captive portal as described in “Configuring the Welcome Screen (Captive Portal)” on page 123.

Notes If you want to configure the Guest and Internal networks on Virtual LAN (VLANs), the switch and DHCP server you are using must support VLANs.

As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard.

Guest Welcome Screen settings are shared among access points across the cluster. When you update these settings for one access point, the configuration will be shared with the other access points in the cluster. For more information about which settings are shared by the cluster and which are not, see "Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?" on page 45.

To configure Internal and Guest networks on virtual LANs, do the following:

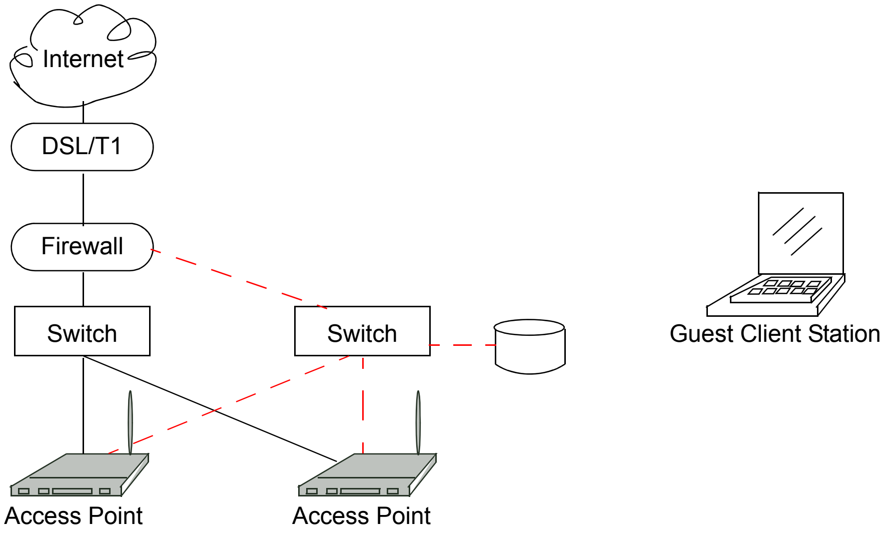
1. Use an Ethernet cable to make a wired connection from the LAN port on the access point to the LAN. (Make sure this port is configured to handle VLAN tagged packets.)

2. Configure **Ethernet (Wired) Settings** for Internal and Guest networks on VLANs as described in "Ethernet (Wired) Settings" on page 89.

   (Start by enabling Guest Access and choosing **For Internal and Guest access, use VLAN on Ethernet Port** as described in "Specifying a Virtual Guest Network" on page 92.)

3. Provide the radio interface settings and network names (SSIDs) for both Internal and Guest networks as described in "Wireless Settings" on page 97.

The figure below shows an example of a Guest network implemented via VLAN; the dotted red lines indicate dedicated guest connections.

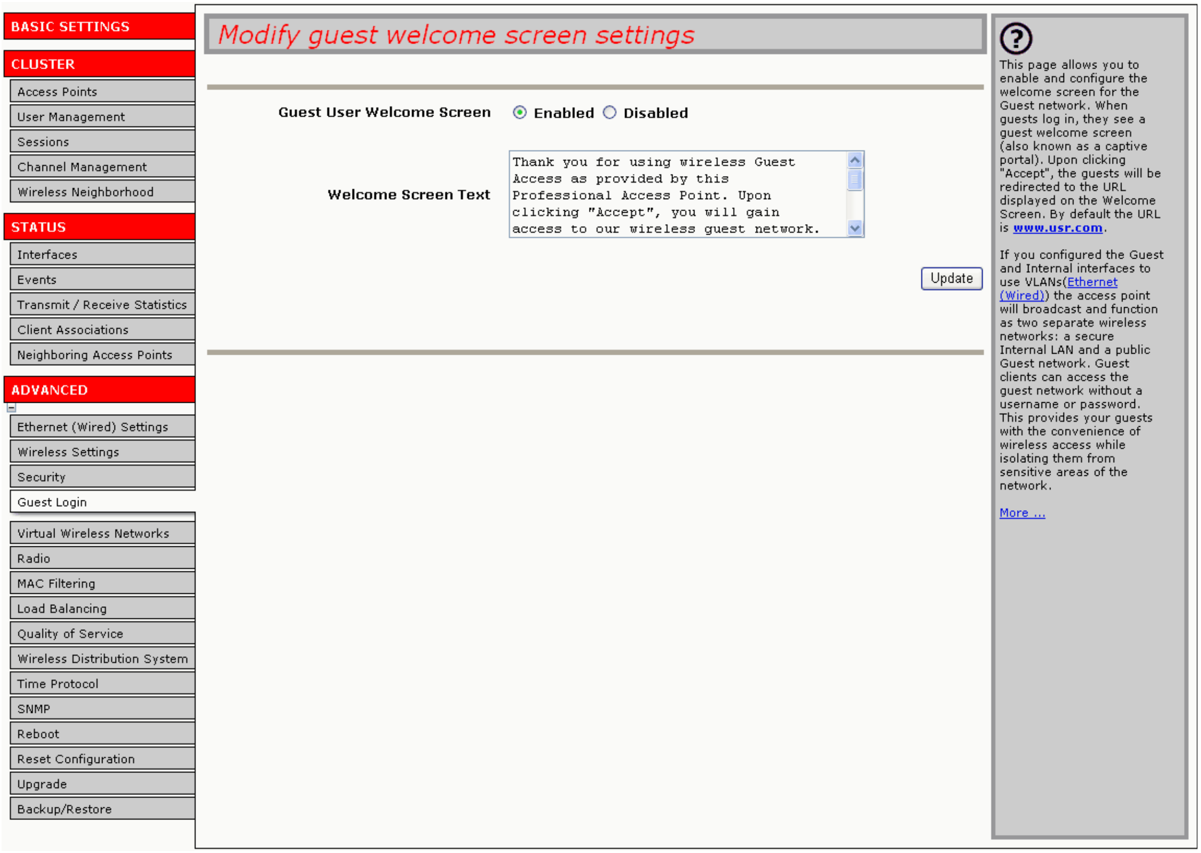


All access points and all connections, including guests, are administered from the same Professional Access Point Web User Interface.

Configuring the Welcome Screen (Captive Portal)

You can set up or modify the Welcome screen that guest clients see when they open a Web browser or try to browse the Web. To set up the captive portal, do the following.

1. Click the Advanced menu's **Guest Login** tab.



Modify guest welcome screen settings

Guest User Welcome Screen ● Enabled ○ Disabled

Welcome Screen Text: Thank you for using wireless Guest Access as provided by this Professional Access Point. Upon clicking "Accept", you will gain access to our wireless guest network.

This page allows you to enable and configure the welcome screen for the Guest network. When guests log in, they see a guest welcome screen (also known as a captive portal). Upon clicking "Accept", the guests will be redirected to the URL displayed on the Welcome Screen. By default the URL is www.usr.com.

If you configured the Guest and Internal interfaces to use VLANs(Ethernet (Wired)) the access point will broadcast and function as two separate wireless networks: a secure Internal LAN and a public Guest network. Guest clients can access the guest network without a username or password. This provides your guests with the convenience of wireless access while isolating them from sensitive areas of the network.

2. Choose **Enabled** to activate the Welcome screen.

3. In the **Welcome Screen Text** field, type the text message that you would like guest clients to see on the captive portal. Note that the default captive portal message directs users to www.usr.com after they click **Accept**:

```
Thank you for using wireless Guest Access as provided by this Professional
Access Point. Upon clicking "Accept", you will gain access to our wireless
guest network. <form action="/accept.cgi" method="POST"><input type="hid-
den" name="URL" value="http://www.usr.com"><center><input type="submit"
name="submit" value="Accept"></center></form>
```

4. Click **Update** to apply the changes.

Using the Guest Network

Once the guest network is configured, a client can access the guest network as follows:

1. A guest client enters an area of coverage and scans for wireless networks.

2. The guest network advertises itself via a Guest SSID or a similar name, depending on how the guest SSID is specified in the Web User Interface for the Guest interface.

3. The guest chooses Guest SSID.

4. The guest starts a Web browser and receives a Guest Welcome screen.

5. The Guest Welcome Screen provides a button for the guest to click to continue.

6. The guest clicks the button and the guest client is enabled to use the guest network.

Configuring Guest Access without Virtual LANs

Configuring a Guest Network on a Dedicated Access Point

To configure an access point dedicated to guest access, you do not have to set up VLANs. All you have to do is configure the Welcome screen as described in “Configuring the Welcome Screen (Captive Portal)” on page 123.

Using the Guest Network

Once the captive portal is enabled on an access point that does not use VLANs, a client can access the guest network as follows:

1. A guest client enters an area of coverage and scans for wireless networks.

2. The guest network advertises itself via a Internal SSID.

3. The guest chooses Internal SSID.

4. The guest starts a Web browser and receives a Guest Welcome screen.

5. The Guest Welcome Screen provides a button for the guest to click to continue.

6. The guest clicks the button and the guest client is enabled to use the guest network.

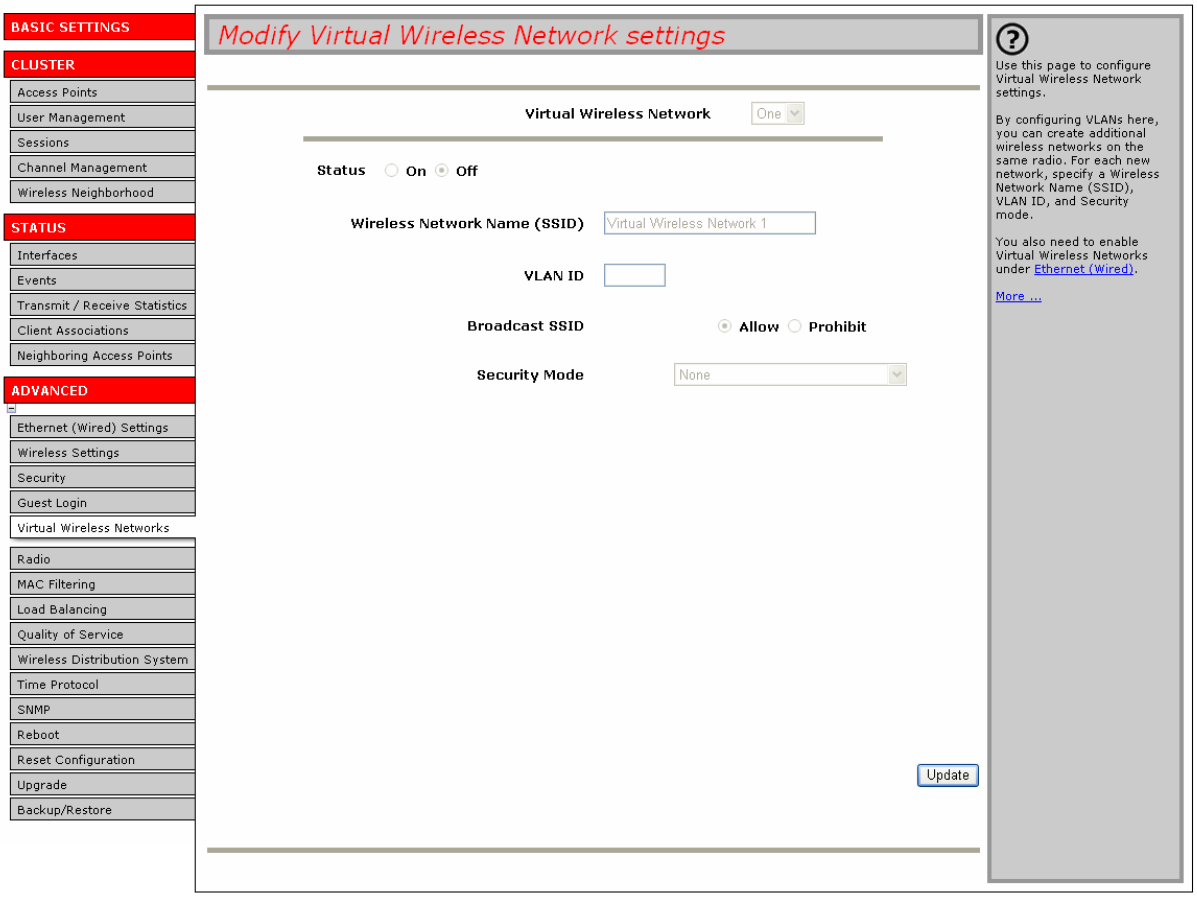
Virtual Wireless Networks

The following sections describe how to configure multiple wireless networks on Virtual LANs (VLANs):

- Navigating to Virtual Wireless Network Settings
- Configuring VLANs
- Updating Settings

Navigating to Virtual Wireless Network Settings

To set up multiple networks on VLANs, click the Advanced menu’s **Virtual Wireless Networks** tab, and update the fields as described below.



Modify Virtual Wireless Network settings

Virtual Wireless Network: One

Status: ○ On ● Off

Wireless Network Name (SSID): Virtual Wireless Network 1

VLAN ID:

Broadcast SSID: ● Allow ○ Prohibit

Security Mode: None

Use this page to configure Virtual Wireless Network settings.

By configuring VLANs here, you can create additional wireless networks on the same radio. For each new network, specify a Wireless Network Name (SSID), VLAN ID, and Security mode.

You also need to enable Virtual Wireless Networks under Ethernet (Wired).

More ...

Configuring VLANs

Notes / Cautions

- To configure additional networks on VLANs, you must first enable Virtual Wireless Networks on the Ethernet (Wired) interface. See “Enabling and Disabling Virtual Wireless Networks on the Access Point” on page 92.
- If you configure VLANs, you may lose connectivity to the access point. First, be sure to verify that the switch and DHCP server you are using can support VLANs per the IEEE 802.1Q standard. After configuring VLANs, physically reconnect the Ethernet cable on the switch to the tagged packet (VLAN) port. Then, reconnect via the Web User Interface to the new IP address. (If necessary, check with the infrastructure support administrator regarding the VLAN and DHCP configurations.)

Field	Description
Virtual Wireless Network	Choose one of the following from the drop-down list to identify an additional network to configure: • **One** • **Two**
Status	You can enable or disable a configured network. • To enable the specified network, click **On**. • To disable the specified network, click **Off**.
Wireless Network Name (SSID)	Enter a name for the wireless network as a character string. This name will apply to all access points on this network. As you add more access points, they will share this SSID. The *Service Set Identifier* (SSID) is an alphanumeric string of up to 32 characters **Note:** If you are connected as a wireless client to the same access point that you are administering, resetting the SSID will cause you to lose connectivity to the access point. You will need to reconnect to the new SSID after you save this new setting.
VLAN ID	Provide a number between 1 and 4094 for the Internal VLAN. This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE 802.1Q frames. The access point must be able to reach the DHCP server. Check with the Administrator regarding the VLAN and DHCP configurations.

Field	Description
Broadcast SSID	Select the **Broadcast SSID** setting by clicking the "Allow" or "Prohibit" radio button. By default, the access point broadcasts (allows) the *Service Set Identifier* (SSID) in its beacon frames. You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the access point's broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client device. Instead, the client must have the exact network name configured in the supplicant before it will be able to connect. **Note:** The Broadcast SSID you set here is specifically for this Virtual Network (One or Two). Other networks continue to use the security modes already configured: your original Internal network (configured on Advanced menu's Ethernet [Wired] page) uses the Broadcast SSID set on Advanced menu's Security page.
Security Mode	Select the **Security Mode** for this VLAN. Select one of the following: • **None** • Static WEP • IEEE 802.1x • WPA/WPA2 Personal (PSK) • WPA/WPA2 Enterprise (RADIUS) **Note:** The Security mode you set here is specifically for this Virtual Network (One or Two). Other networks continue to use the security modes already configured: • Your original Internal network uses the Security mode set on the Advanced menu's Security page. • If a Guest VLAN is configured, it always uses **None**. For a comparison of the available security modes, see "How Do I Know Which Security Mode to Use?" on page 101.

Updating Settings

To apply your changes, click **Update**.

Radio

The following sections describe how to configure Radio Settings on the Professional Access Point:

- Understanding Radio Settings
- Navigating to Radio Settings
- Configuring Radio Settings
- Updating Settings

Understanding Radio Settings

Radio settings directly control the behaviour of the radio device in the access point and its interaction with the physical medium, that is, how and what type of electromagnetic waves the access point emits. You can specify whether the radio is on or off, radio frequency (RF) broadcast channel, beacon interval (amount of time between access point beacon transmissions), transmit power, IEEE 802.11 mode in which the radio operates, and so on.

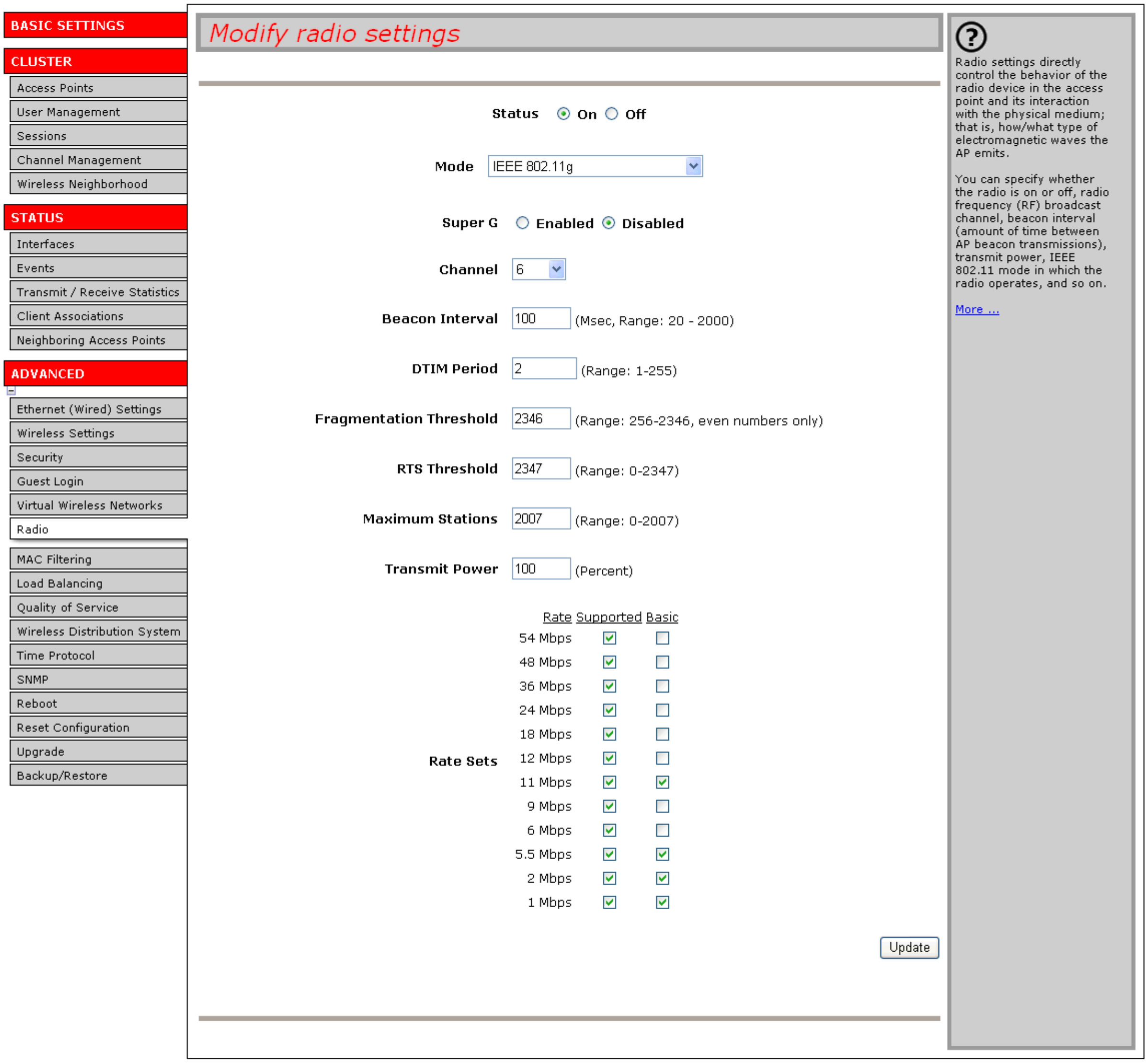
The Professional Access Point can broadcast in the following modes:

- IEEE 802.11b
- IEEE 802.11g

The IEEE mode along with other radio settings are configured as described in “Navigating to Radio Settings” on page 130 and “Configuring Radio Settings” on page 130.

Navigating to Radio Settings

To specify radio settings, click the Advanced menu's **Radio** tab, and update the fields as described below.



Modify radio settings

Status ● On ○ Off

Mode IEEE 802.11g

Super G ○ Enabled ● Disabled

Channel 6

Beacon Interval 100 (Msec, Range: 20 - 2000)

DTIM Period 2 (Range: 1-255)

Fragmentation Threshold 2346 (Range: 256-2346, even numbers only)

RTS Threshold 2347 (Range: 0-2347)

Maximum Stations 2007 (Range: 0-2007)

Transmit Power 100 (Percent)

Rate Sets

Rate	Supported	Basic
54 Mbps	☑	☐
48 Mbps	☑	☐
36 Mbps	☑	☐
24 Mbps	☑	☐
18 Mbps	☑	☐
12 Mbps	☑	☐
11 Mbps	☑	☑
9 Mbps	☑	☐
6 Mbps	☑	☐
5.5 Mbps	☑	☑
2 Mbps	☑	☑
1 Mbps	☑	☑

Radio settings directly control the behavior of the radio device in the access point and its interaction with the physical medium; that is, how/what type of electromagnetic waves the AP emits.

You can specify whether the radio is on or off, radio frequency (RF) broadcast channel, beacon interval (amount of time between AP beacon transmissions), transmit power, IEEE 802.11 mode in which the radio operates, and so on.

Configuring Radio Settings

Field	Description
Status (On/Off)	Specify whether you want the radio on or off by clicking **On** or **Off**.

Field	Description
Mode	The *Mode* defines the *Physical Layer* (PHY) standard being used by the radio. Select one of these modes: • **IEEE 802.11b** • **IEEE 802.11g** (the default). This mode allows both 802.11b and 802.11g clients to connect to the access point. To enable 802.11g clients only and deny acces to 802.11b clients, select a **Basic** rate that is not supported by 802.11b, such as 6Mbps. Basic rate options appear at the bottom of the Radio tab.
Super G	Enabling Super G provides better performance by increasing radio throughput for a radio mode. Keep in mind that with Super G enabled the access point transmissions will consume more bandwidth. • To enable Super G click **Enabled**. • To disable Super G click **Disabled**.
Channel	The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. For most Modes, the default is **Auto**. Auto is the recommended mode because it automatically detects the best channel choices based on signal strength, traffic loads, and so on.
Beacon Interval	The *Beacon Interval* value is set in milliseconds. Enter a value within the range 20–2000. Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behaviour is to send a beacon frame once every 100 milliseconds (or 10 per second).
DTIM Period	Specify a DTIM period within the range 1–255. The *Delivery Traffic Information Map* (DTIM) message is an element included in some Beacon frames. It indicates which clients, currently sleeping in low-power mode, have data buffered on the access point awaiting pickup. The DTIM period you specify here indicates how often the clients served by this access point will check for buffered data still on the access point awaiting pickup. The measurement is the count of beacons. For example, if you set the DTIM period to 1, clients will check for buffered data on the access point at every beacon. If you set this to 10, clients will check at every 10th beacon.

Field	Description
Fragmentation Threshold	Specify a number within the range 256–2,346 to set the frame size threshold in bytes. The *fragmentation threshold* is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames. If the packet being transmitted is equal to or less than the threshold, fragmentation will not be used. Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation. Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help *improve* network performance and reliability if properly configured. Sending smaller frames (by using lower fragmentation threshold) may help with some interference problems; for example, with microwave ovens. By default, fragmentation is off. USRobotics recommends not using fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.
RTS Threshold	Specify an RTS Threshold value within the range 0–2347. The RTS threshold specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.
Maximum Stations	Enter a value within the range 0–2007. Specify the maximum number of stations allowed to access this access point at any one time.

Field	Description
Transmit Power	Provide a percentage value to set the transmit power for this access point. The default is to have the access point transmit using 100 percent of its power. Recommendations: • For most cases, USRobotics recommends using the default and having the transmit power set to 100 percent. This is more cost-efficient because it gives the access point a maximum broadcast range and reduces the number of APs needed. • To increase capacity of the network, place APs closer together and reduce the value of the transmit power. This will help reduce overlap and interference among APs. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.
Rate Sets	Select the transmission rate sets that you want the access point to support and the basic rate sets you want the access point to advertise. Rates are expressed in megabits per second. • **Supported Rate Sets** indicate rates that the access point supports. You can select multiple rates. The access point will automatically choose the most efficient rate based on factors like error rates and distance of clients from the access point. • **Basic Rate Sets** indicate rates that the access point will advertise to the network for the purposes of setting up communication with other APs and clients on the network. It is generally more efficient to have an access point broadcast a subset of its supported rate sets. The highest basic rate selected is also the access point's multicast rate. To transmit multicast packets at a higher rate than the default of 11Mbps, select a higher **Basic** Rate.

Updating Settings

To apply your changes, click **Update**.

MAC Filtering

A *Media Access Control* (MAC) address is a hardware address that uniquely identifies each node of a network. All IEEE 802 network devices share a common 48-bit MAC address format, usually displayed as a string of 12 hexadecimal digits separated by colons, for example `FE:DC:BA:09:87:65`.

Each wireless network interface card (NIC) used by a wireless client has a unique MAC address.

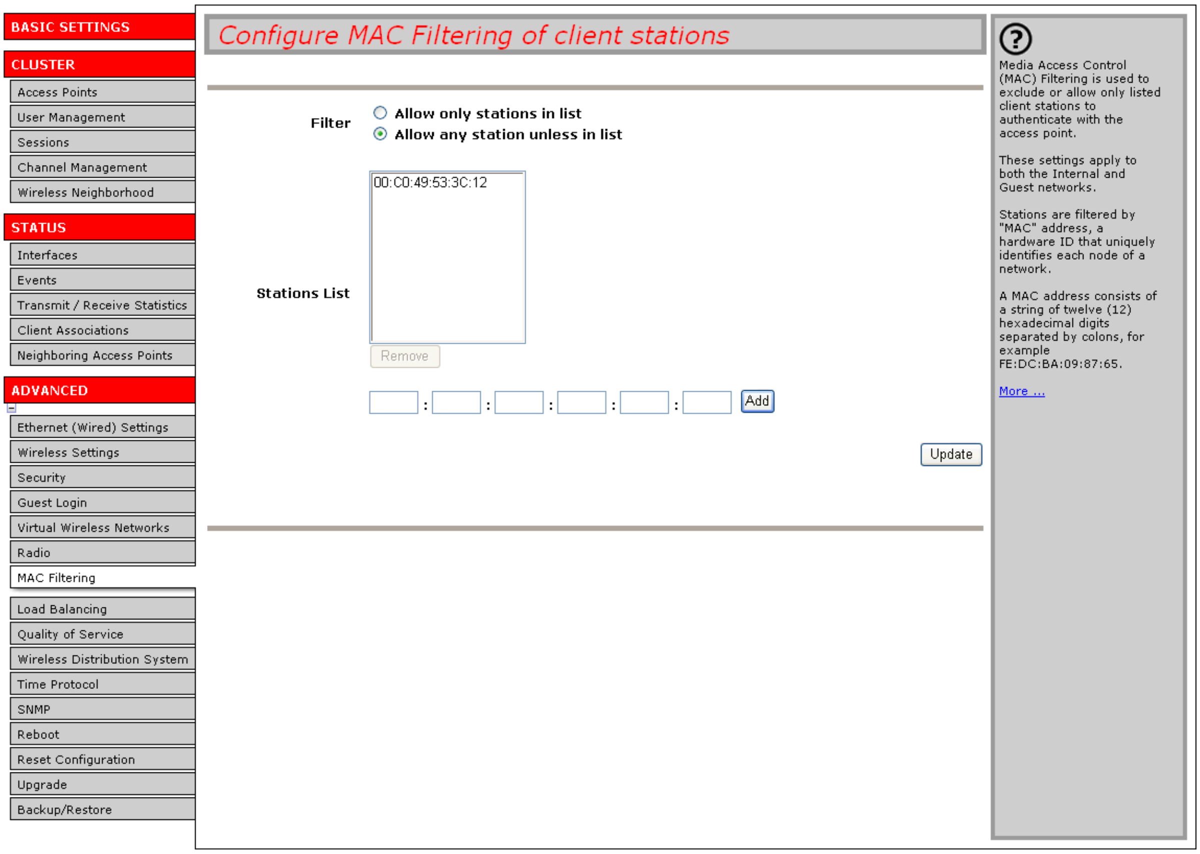
You can control client access to your wireless network by switching on MAC Filtering and specifying a list of approved MAC addresses. When MAC Filtering is on, only clients with approved MAC addresses can access the network.

The following sections describe how to use MAC address filtering on the Professional Access Point:

- Navigating to MAC Filtering Settings
- Using MAC Filtering
- Updating Settings

Navigating to MAC Filtering Settings

To enable filtering by MAC address, click the Advanced menu's **MAC Filtering** tab, and update the fields as described below.



Configure MAC Filtering of client stations

Filter ○ Allow only stations in list
● Allow any station unless in list

Stations List: 00:C0:49:53:3C:12

Media Access Control (MAC) Filtering is used to exclude or allow only listed client stations to authenticate with the access point.

These settings apply to both the Internal and Guest networks.

Stations are filtered by "MAC" address, a hardware ID that uniquely identifies each node of a network.

A MAC address consists of a string of twelve (12) hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

Using MAC Filtering

This page allows you to control access to Professional Access Point based on *Media Access Control* (MAC) addresses. You can choose to *allow* access by listed MAC addresses or *prevent* access by listed MAC addresses.

For the Guest interface, MAC Filtering settings apply to both BSSes.

Field	Description
Filter	To set the MAC Address Filter, select one of the following options: • **Allow only stations in the list** • **Allow any station unless in list**

Field	Description
Stations List	To add a MAC Address to the Stations List, type the 48-bit MAC address into the lower text boxes, then click **Add**. The MAC Address is added to the Stations List. To remove a MAC Address from the Stations List, select its 48-bit MAC address, then click **Remove**. The stations in the list will be either allowed to access or prevented from accessing the access point depending on the value that you chose for **Filter**.

Updating Settings

To apply your changes, click **Update**.

Load Balancing

The Professional Access Point allows you to balance the distribution of wireless client connections across multiple access points. Using load balancing, you can prevent the performance degradation that results when a single access point handles a disproportionate share of the wireless traffic.

The following sections describe how to configure Load Balancing on your wireless network:

- Understanding Load Balancing
  - Identifying the Imbalance: Overworked or Under-utilized Access Points
  - Specifying Limits for Utilization and Client Associations
  - Load Balancing and QoS
- Navigating to Load Balancing Settings
- Configuring Load Balancing
- Updating Settings

Understanding Load Balancing

Like most configuration settings on the Professional Access Point, load balancing settings are shared among clustered access points.

Note In some cases you might want to set limits for only one access point that is consistently over-utilized. You can apply unique settings to an access point if it is operating in standalone mode. (See “Understanding Clustering” on page 44 and “Navigating to Access Points Management” on page 44.)

Identifying the Imbalance: Overworked or Under-utilized Access Points

Comparison of Sessions data for multiple access points allows you to identify an access point that is consistently handling a disproportionately large percentage of wireless traffic. This can happen when location placement or other factors cause one access point to transmit the strongest signal to a majority of clients on a network. By default, that access point will receive most of client requests while the other access points stay idle much of the time.

Imbalances in distribution of wireless traffic across access points will be evident in Sessions statistics, which will show higher utilization rates on overworked APs and higher Idle times on under-utilized APs. An access point that is handling a disproportionate amount of traffic might also show slower data rates or lower transmit and receive rates due to the overload.

Specifying Limits for Utilization and Client Associations

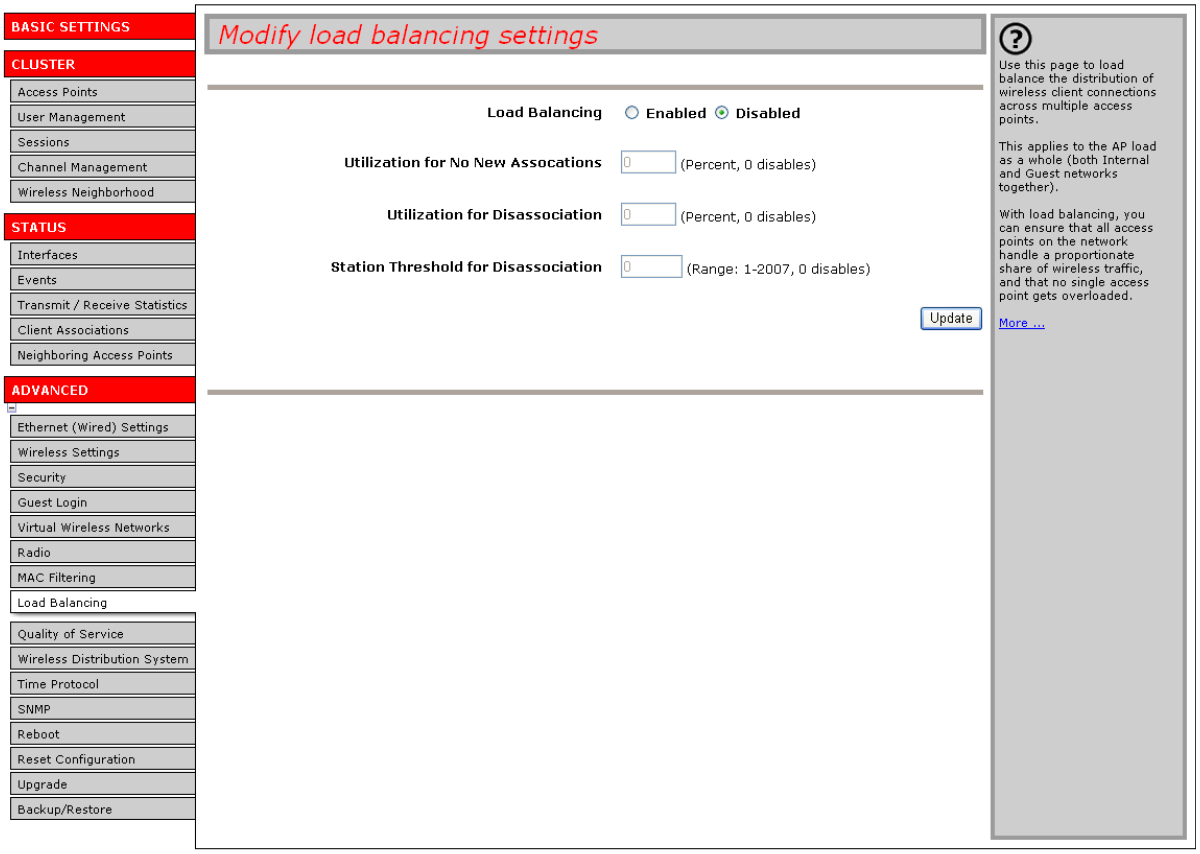
You can correct for imbalances in network access point utilization by enabling load balancing and setting limits on utilization rates and number of client associations allowed per access point.

Load Balancing and QoS

Load balancing contributes to *Quality of Service* (QoS) for *Voice Over IP* (VoIP) and other such time-sensitive applications competing for bandwidth and timely access to the air waves on a wireless network. For more information about configuring your network for QoS, see “Quality of Service” on page 143.

Navigating to Load Balancing Settings

In the Web User Interface, click the Advanced menu’s **Load Balancing** tab, and update the fields as described in the next section.



Modify load balancing settings

Load Balancing ○ Enabled ● Disabled

Utilization for No New Assocations 0 (Percent, 0 disables)

Utilization for Disassociation 0 (Percent, 0 disables)

Station Threshold for Disassociation 0 (Range: 1-2007, 0 disables)

Use this page to load balance the distribution of wireless client connections across multiple access points.

This applies to the AP load as a whole (both Internal and Guest networks together).

With load balancing, you can ensure that all access points on the network handle a proportionate share of wireless traffic, and that no single access point gets overloaded.

Configuring Load Balancing

To configure load balancing, enable **Load Balancing** and set limits and behaviour to be triggered by a specified utilization rate of the access point.

Note

- To view the current Utilization Rates for access points, click the Cluster menu's Sessions tab. (See "Sessions" on page 59.)
- When clients are disassociated from an access point, the network will provide continuous service if another access point is within range of the client. Clients should automatically retry the access points to which they were originally connected and then try other APs on the subnet. Clients who are disassociated from one access point will experience a seamless transition to another access point on the same subnet.
- Load Balancing settings apply to the access point load as a whole. When Guest access is enabled, the settings apply to both Internal and Guest networks together.

Field	Description
Load Balancing	To enable load balancing on this access point, click **Enable**. To disable load balancing on this access point, click **Disable**.
Utilization for No New Associations	Utilization rate limits relate to wireless bandwidth utilization. Provide a bandwidth utilization rate percentage limit for this access point to indicate when to stop accepting new client associations. When the utilization rate for this access point exceeds the specified limit, no new client associations will be allowed on this access point. If you specify 0 in this field, all new associations will be allowed regardless of the utilization rate.
Utilization for Disassociation	Utilization rate limits relate to wireless bandwidth utilization. Provide a bandwidth utilization rate percentage limit for this access point to indicate when to disassociate current clients. When the utilization rate exceeds the specified limit, a client currently associated with this access point will be disconnected. If you specify 0 in this field, current clients will never be disconnected regardless of the utilization rate.
Stations Threshold for Disassociation	Specify the number of clients that you want as a stations threshold for disassociation. If the number of clients associated with the access point at any one time is equal to or less than the number you specify here, no client will be disassociated regardless of the **Utilization for Disassociation** value. Theoretically, the maximum number of clients allowed is 2007. ▶ USRobotics recommends setting the maximum to between 30 and 50 clients . This allows for a workable load on the access point, given that bandwidth is shared among the access point clients.

Updating Settings

To apply your changes, click **Update Settings**.

Quality of Service

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like *Voice-over-IP* (VoIP); other types of audio, video, and streaming media; and traditional IP data.

The following sections describe how to configure Quality of Service queues on the Professional Access Point:

- Understanding QoS
  - QoS and Load Balancing
  - 802.11e and WMM Standards Support
  - QoS Queues and Parameters to Coordinate Traffic Flow
- Navigating to QoS Settings
- Configuring QoS Queues
  - Configuring AP EDCA Parameters
  - Enabling/Disabling Wi-Fi Multimedia
  - Configuring Station EDCA Parameters
- Updating Settings

Understanding QoS

A primary factor that affects QoS is network congestion due to an increased number of clients attempting to access the air waves and higher traffic volume competing for bandwidth during a busy time of day. The most noticeable degradation in service on a busy, overloaded network will be evident in time-sensitive applications like video, *Voice-over-IP* (VoIP), and streaming media.

Unlike typical data files, which are less affected by variability in QoS, video, VoIP and streaming media must be sent in a specific order at a consistent rate and with minimum delay between Packet transmissions. If the quality of service is compromised, the audio or video will be distorted.

QoS and Load Balancing

By using a combination of load balancing (see “Load Balancing” on page 139) and QoS techniques, you can provide a high quality of service for time-sensitive applications, even on a busy network. Load balancing is a way of better distributing the traffic volume across access points. QoS is a means of allocating bandwidth and network access based on transmission priorities for different types of wireless traffic within a single access point.

802.11e and WMM Standards Support

QoS describes a range of technologies for controlling data streams on shared network connections. The

IEEE 802.11e task group is in the process of defining a QoS standard for transmission quality and availability of service on wireless networks. QoS is designed to provide better network service by minimizing network congestion; limiting Jitter, Latency, and Packet Loss; supporting dedicated bandwidth for time-sensitive or mission critical applications; and prioritising wireless traffic for channel access.

As with all IEEE 802.11 working group standards, the goal is to provide a standard way of implementing QoS features so that components from different companies are interoperable.

The Professional Access Point provides QoS based on the *Wireless Multimedia* (WMM) specification and *Wireless Multimedia* (WMM) standards, which are implementations of a subset of 802.11e features.

Both access points and wireless clients can be WMM-enabled.

QoS Queues and Parameters to Coordinate Traffic Flow

Configuring QoS options on the Professional Access Point consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for voice, video, multimedia, and mission-critical applications and rely on best-effort parameters for traditional IP data.

For example, time-sensitive voice, video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data—which are less time-sensitive but often more data-intensive—are expected to tolerate longer wait times.

The Professional Access Point implementation of QoS is based on the IEEE Wireless Multimedia (WMM) standard. A Linux-based queuing class is used to tag packets and establish multiple queues. The queues provided offer built-in prioritisation and routing based on the type of data being transmitted.

The Web User Interface provides a way for you to configure parameters on the queues.

QoS Queues and Type of Service (ToS) on Packets

QoS on the Professional Access Point uses WMM information in the IP packet header related to Type of Service (ToS). Every IP packet sent over the network includes a ToS field in the header that indicates how the data is to be prioritised and transmitted over the network. The ToS field consists of a 3- to 7-bit value with each bit representing a different aspect or degree of priority for this data as well as other meta-information (low delay, high throughput, high reliability, low cost, and so on).

For example, the ToS for FTP data packets is likely to be set for maximum throughput since the critical consideration for FTP is the ability to transmit bulk data. Interactive feedback is a benefit in this situation but certainly is less critical than the FTP data itself. VoIP data packets are set for minimum delay because time is a critical factor in quality and performance for that type of data.

The access point examines the ToS field in the header of each packet that passes through the access point. Based on the value in a packet's ToS field, the access point prioritises the packet for transmission by assigning it to one of the queues. This process occurs automatically, regardless of whether you deliberately configure QoS or not.

A different type of data is associated with each queue. The queue and associated priorities and parameters for transmission are as follows:

- **Data 0 (Voice)**. Highest priority queue, minimum delay. Time-sensitive data such as Voice over IP (VoIP) is automatically sent to this queue.

- **Data 1 (Video)**. High priority queue, minimum delay. Time-sensitive data such as Video and other streaming media are automatically sent to this queue.

- **Data 2 (Best Effort)**. Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

- **Data 3 (Background)**. Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

Packets in a higher priority queue will be transmitted before packets in a lower priority queue. Interactive data in the queues labeled "Data 0" and "Data 1" is always sent first, best effort data in "Data 2" is sent next, and Background (bulk) data in "Data 3" is sent last. Each lower-priority queue (class of traffic) gets bandwidth that is left over after the higher classes of traffic have been sent. At an extreme end if you have enough interactive data to keep the access point busy all the time, low priority traffic would never get sent.

Using the QoS settings in the Web User Interface, you can configure *Enhanced Distributed Channel Access* (EDCA) parameters that determine how each queue is treated when it is sent by the access point to the client or by the client to the access point.

Note Wireless traffic travels:

- Downstream from the access point to the client
- Upstream from client to access point
- Upstream from access point to network
- Downstream from network to access point

With WMM enabled, QoS settings on the Professional Access Point affect the first two of these; *downstream* traffic flowing from the access point to client (access point EDCA parameters) and the *upstream* traffic flowing from the client to the access point (station EDCA parameters).

With WMM disabled, you can still set some parameters on the downstream traffic flowing from the access point to the client (access point EDCA parameters).

Traffic flow to and from the network is not under control of the QoS settings on the access point.

EDCF Control of Data Frames and Arbitration Interframe Spaces

Data is transmitted over 802.11 wireless networks in *frames*. A *Frame* consists of a discrete portion of data along with descriptive meta-information packaged for transmission on a wireless network.

Note A Frame is similar in concept to a *Packet*, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).

Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection.

The 802.11 standard defines various frame types for management and control of the wireless infrastructure, and for data transmission. 802.11 frame types are (1) *management frames*, (2) *control frames*, and (3) *data frames*. Management and control frames, which manage and control the availability of the wireless infrastructure, automatically have higher priority for transmission.

802.11e uses *interframe spaces* to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data.

Management and control frames wait a minimum amount of time for transmission: they wait a *short interframe space* (SIF). These wait times are built into 802.11 as infrastructure support and are not configurable.

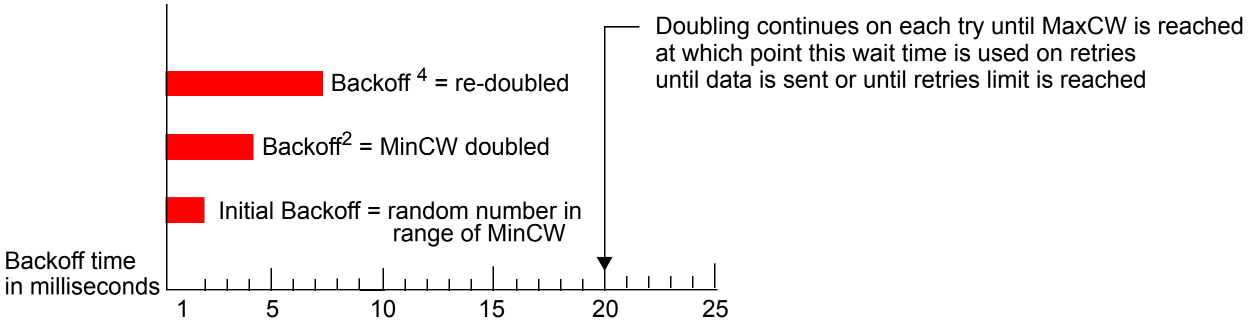
The Professional Access Point supports the *Enhanced Distribution Coordination Function* (EDCF) as defined by the 802.11e standard. EDCF, which is an enhancement to the DCF standard and is based on CSMA/CA protocol, defines the interframe space (IFS) between *data frames*. Data frames wait for an amount of time defined as the *arbitration interframe space* (AIFS) before transmitting. The AIFS parameter is configurable.

(Note that sending data frames in AIFS allows higher priority management and control frames to be sent in SIFs first.)

The AIFS ensures that multiple access points do not try to send data at the same time but instead wait until a channel is free.

Random Backoff and Minimum / Maximum Contention Windows

If an access point detects that the medium is in use, it uses the DCF *random backoff* timer to determine the amount of time to wait before attempting to access a given channel again. Each access point waits a random period of time between retries. The wait time (initially a random value within a range specified as the *Minimum Contention Window*) increases exponentially up to a specified limit (*Maximum Contention Window*). The random delay avoids most of the collisions that would occur if multiple APs got access to the medium at the same time and tried to transmit data simultaneously. The greater the number of active users on a network, the more significant the performance gains of the backoff timer will be due to the reduction in the number of collisions and retransmissions.


Doubling continues on each try until MaxCW is reached
at which point this wait time is used on retries
until data is sent or until retries limit is reached
Backoff 4 = re-doubled
Backoff2 = MinCW doubled
Initial Backoff = random number in
range of MinCW
Backoff time
in milliseconds
1
5
10
15
20
25

The random backoff used by the access point is a configurable parameter. To describe the random delay, a Minimum Contention Window (**cwMin**) and a Maximum Contention Window (**cwMax**) is defined.

- The value specified for the Minimum Contention Window is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.

- If the first random backoff time ends before successful transmission of the data frame, the access point increments a retry counter, and doubles the value of the random backoff window. The value specified in the Maximum Contention Window is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

Packet Bursting for Better Performance

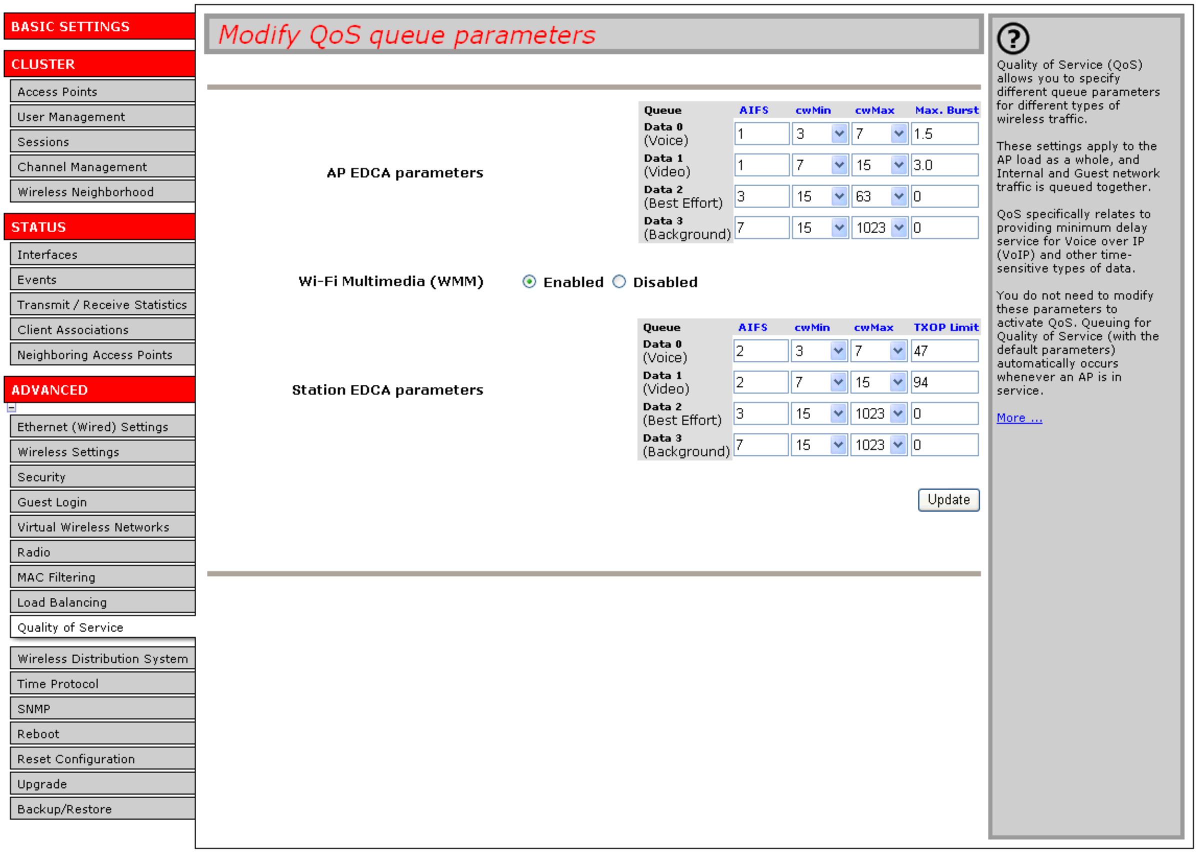
The Professional Access Point includes 802.11e based *packet bursting* technology that increases data throughput and speed of transmission over the wireless network. Packet bursting enables the transmission of multiple packets without the extra overhead of header information. The effect of this is to increase network speed and data throughput. The size of packet bursts allowed (maximum burst length) is a configurable parameter.

Transmission Opportunity (TXOP) Interval for Client Stations

The *Transmission Opportunity* (TXOP) is an interval of time when a Wi-Fi Multimedia (WMM) client station has the right to initiate transmissions onto the wireless medium (WM).

Navigating to QoS Settings

To set up queues for QoS, click the Advanced menu’s **Quality of Service** tab, and configure settings as described below.



Modify QoS queue parameters

AP EDCA parameters

Queue	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Voice)	1	3	7	1.5
Data 1 (Video)	1	7	15	3.0
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Wi-Fi Multimedia (WMM) ● Enabled ○ Disabled

Station EDCA parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

Quality of Service (QoS) allows you to specify different queue parameters for different types of wireless traffic.

These settings apply to the AP load as a whole, and Internal and Guest network traffic is queued together.

QoS specifically relates to providing minimum delay service for Voice over IP (VoIP) and other time-sensitive types of data.

You do not need to modify these parameters to activate QoS. Queuing for Quality of Service (with the default parameters) automatically occurs whenever an AP is in service.

Configuring QoS Queues

Configuring Quality of Service (QoS) on the Professional Access Point consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (via *Contention Windows*) for transmission. The settings described here apply to data transmission behaviour on the access point only, not to that of the client stations.

Notes

- For the Guest interface, QoS queue settings apply to the access point load as a whole (both BSSes together).
- Internal and Guest network traffic is always queued together.

Configuring Quality of Service includes:

- Configuring AP EDCA Parameters
- Enabling/Disabling Wi-Fi Multimedia
- Updating Settings

Configuring AP EDCA Parameters

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station.

Field	Description
Queue	Queues are defined for different types of data transmitted from the access point-to the client station: **Data 0 (Voice)** Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. **Data 1(Video)** Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. **Data 2 (best effort)** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. **Data 3 (Background)** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). For more information, see “QoS Queues and Parameters to Coordinate Traffic Flow” on page 144.
AIFS **(Inter-Frame Space)**	The *Arbitration Inter-Frame Spacing* (**AIFS**) specifies a wait time in milliseconds for data frames. Valid values for AIFS are 1 through 255. For more information, see “EDCF Control of Data Frames and Arbitration Interframe Spaces” on page 145.

Field	Description
cwMin **(Minimum Contention Window)**	This parameter is input to the algorithm that determines the initial random backoff wait time for retry of a transmission. Select a value from the list. The value selected for **cwMin** is the upper limit, in milliseconds, of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified in **cwMin**. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. For more information, see "Random Backoff and Minimum / Maximum Contention Windows" on page 146.
cwMax **(Maximum Contention Window)**	Select a value that is higher than **cwMin**. The value specified for **cwMax** is the upper limit, in milliseconds, for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. For more information, see "Random Backoff and Minimum / Maximum Contention Windows" on page 146.
Max. Burst **(Maximum Burst Length)**	**AP EDCA Parameter Only**. The **Max. Burst Length** applies only to traffic flowing from the access point to the client station. This value specifies, in milliseconds, the Maximum Burst Length allowed for packet bursts on the wireless network. A *packet burst* is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Valid values for maximum burst length are 0.0 through 999.9. For more information, see "Packet Bursting for Better Performance" on page 147.

Enabling/Disabling Wi-Fi Multimedia

By default, Wi-Fi MultiMedia (WMM) is enabled on the access point. With WMM enabled, QoS prioritisation and coordination of wireless medium access is on. With WMM enabled, QoS settings on the Professional Access Point control *downstream* traffic flowing from the access point to client station (access point EDCA parameters) and the *upstream* traffic flowing from the station to the access point (station EDCA parameters).

Disabling WMM will deactivate QoS control of station EDCA parameters on *upstream* traffic flowing from the station to the access point

With WMM disabled, you can still set some parameters on the downstream traffic flowing from the access point to the client station (access point EDCA parameters).

- To disable WMM extensions, click **Disabled**.

- To enable WMM extensions, click **Enabled**.

Configuring Station EDCA Parameters

Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point.

Field	Description
Queue	Queues are defined for different types of data transmitted from the client station to the access point: **Data 0 (Voice)** Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. **Data 1(Video)** Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. **Data 2 (best effort)** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. **Data 3 (Background)** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). For more information, see “QoS Queues and Parameters to Coordinate Traffic Flow” on page 144.
AIFS **(Inter-Frame Space)**	The *Arbitration Inter-Frame Spacing* (AIFS) specifies a wait time (in milliseconds) for *data frames*. For more information, see “EDCF Control of Data Frames and Arbitration Interframe Spaces” on page 145.

Field	Description
cwMin **(Minimum Contention Window)**	This parameter is input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. The value specified here in the *Minimum Contention Window* is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. For more information, see “Random Backoff and Minimum / Maximum Contention Windows” on page 146.
cwMax **(Maximum Contention Window)**	The value specified here in the *Maximum Contention Window* is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. For more information, see “Random Backoff and Minimum / Maximum Contention Windows” on page 146.
TXOP Limit **(Transmission Opportunity Limit)**	**Station EDCA Parameter Only** (The TXOP Limit applies only to traffic flowing from the client station to the access point.) The *Transmission Opportunity* (TXOP) is an interval of time when a WME client station has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the *Transmission Opportunity* (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.

Updating Settings

To apply your changes, click **Update**.

Wireless Distribution System

The Professional Access Point lets you connect multiple access points using a Wireless Distribution System (WDS). WDS allows access points to communicate with one another wirelessly in a standardized way. This capability is critical to providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.

The following sections describe how to configure the WDS on the Professional Access Point:

- Understanding the Wireless Distribution System
  - Using WDS to Bridge Distant Wired LANs
  - Using WDS to Extend the Network Beyond the Wired Coverage Area
  - Backup Links and Unwanted Loops in WDS Bridges
  - Security Considerations Related to WDS Bridges
- Navigating to WDS Settings
- Configuring WDS Settings
  - Example of Configuring a WDS Link
- Updating Settings

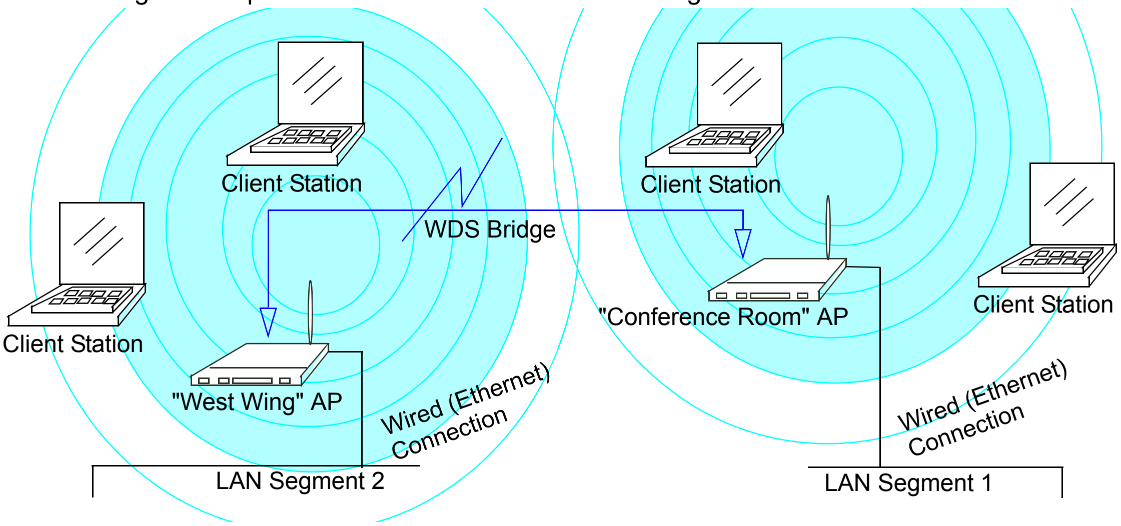
Understanding the Wireless Distribution System

A *Wireless Distribution System* (WDS) is an 802.11f technology that wirelessly connects access points, known as Basic Service Sets (BSS), to form what is known as an *Extended Service Set* (ESS).

Note A BSS generally equates to an access point deployed as a single-access-point wireless network. In cases where multi-BSSID features make a single access point look like two or more access points to the network, the access point has multiple unique BSSIDs.

Using WDS to Bridge Distant Wired LANs

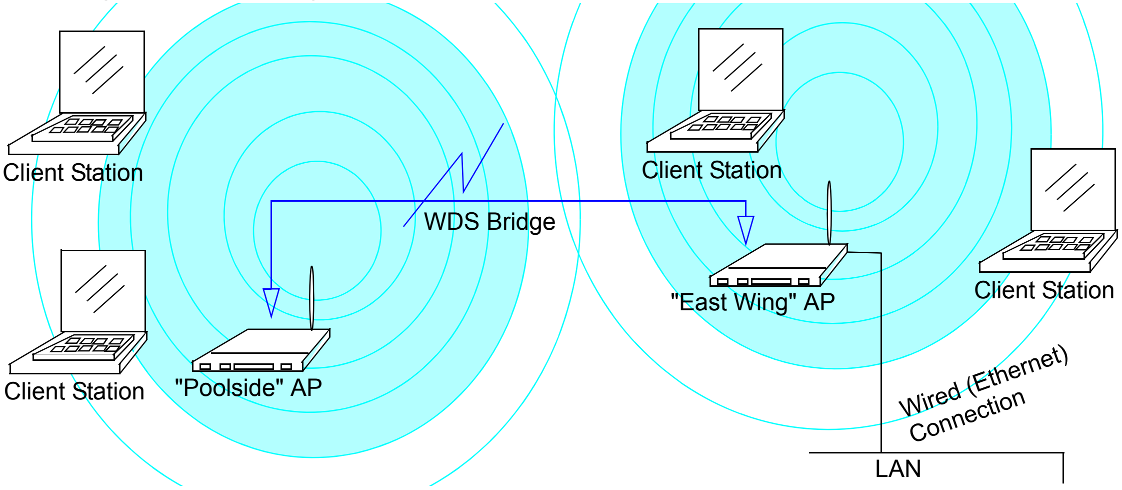
In an ESS—a network of multiple access points—each access point serves part of an area that is too large for a single access point to cover. You can use WDS to bridge distant Ethernets to create a single LAN. For example, suppose that you have one access point that is connected to the network by Ethernet and serving multiple clients in the Conference Room (LAN Segment 1), and another Ethernet-wired access point serving stations in the West Wing offices (LAN Segment 2). You can bridge the Conference Room and West Wing access points with a WDS link to create a single network for clients in both areas.



Using WDS to Extend the Network Beyond the Wired Coverage Area

An ESS can extend the reach of the network into areas where cabling would be difficult, costly, or inefficient.

For example, suppose you have an access point which is connected to the network by Ethernet and serving multiple clients in one area ("East Wing" in this example) but cannot reach other clients which are out of range. Suppose also that it is too difficult or too costly to wire the distant area with Ethernet cabling. You can solve this problem by placing a second access point closer to second group of stations ("Poolside" in this example) and bridge the two APs with a WDS link. This *extends* your network wirelessly by providing an extra hop to get to distant stations.



Backup Links and Unwanted Loops in WDS Bridges

Another use for WDS bridging, the creation of backup links, is not supported by the Professional Access Point. The topic is included here to emphasize that you should not try to use WDS in this way; backup links will result in unwanted, endless loops of data traffic.

If an access point provides *Spanning Tree Protocol* (STP), WDS can be used to configure backup paths between access points across the network. For example, between two access points you could have both a primary path via Ethernet and a secondary (backup) wireless path via a WDS link. If the Ethernet connection goes down, STP would reconfigure its map of the network and effectively fix the down network segment by activating the backup wireless path.

The Professional Access Point does not provide STP. Without STP, it is possible that both connections, or paths, may be active at the same time, resulting in an endless loop of traffic on the LAN.

Therefore, be sure not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges.

For more information, see the "Do not create loops" note under “Configuring WDS Settings” on page 156.

Security Considerations Related to WDS Bridges

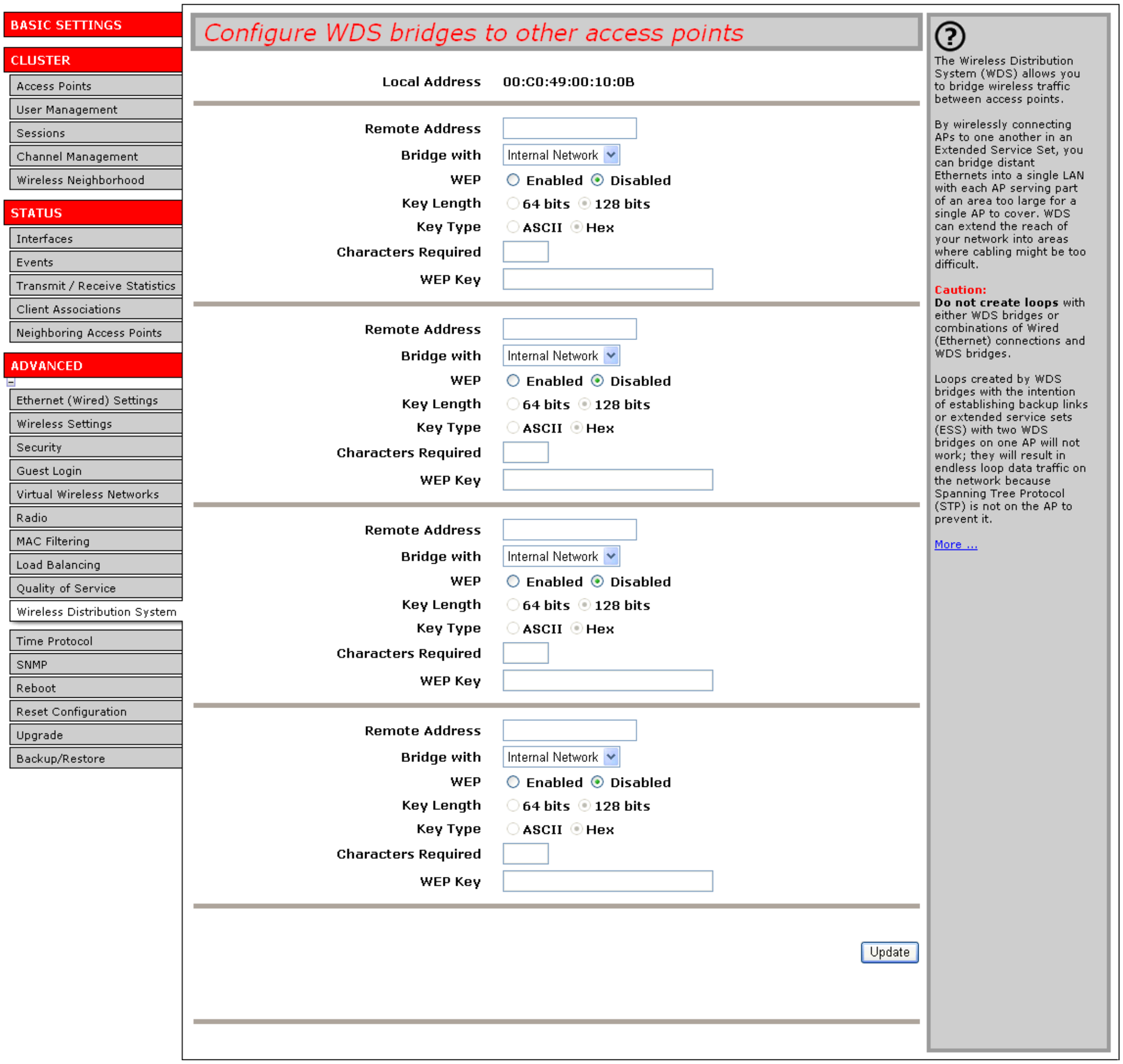
Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. Both access points in a given WDS link must be configured with the same WDS security settings. For static WEP, either a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key is specified for data encryption.

You can enable Static WEP on the WDS link (bridge). When WEP is enabled, all data exchanged between the two access points in a WDS link is encrypted using a fixed WEP key that you provide. USRobotics recommends using Static WEP for your WDS link and the highest level of security available for the individual client networks that you are bridging.

For more information about the effectiveness of different security modes, see “Security” on page 101. This topic also covers use of **None** as the security mode for access-point-to-station traffic on the Guest network, which is intended for less sensitive data traffic.

Navigating to WDS Settings

To specify the details of traffic exchange from this access point to others, click the Advanced menu’s **Wireless Distribution System** tab, and update the fields as described below.



Configure WDS bridges to other access points

Local Address 00:C0:49:00:10:0B

Remote Address
Bridge with Internal Network
WEP ○ Enabled ● Disabled
Key Length ○ 64 bits ● 128 bits
Key Type ○ ASCII ● Hex
Characters Required
WEP Key

Remote Address
Bridge with Internal Network
WEP ○ Enabled ● Disabled
Key Length ○ 64 bits ● 128 bits
Key Type ○ ASCII ● Hex
Characters Required
WEP Key

Remote Address
Bridge with Internal Network
WEP ○ Enabled ● Disabled
Key Length ○ 64 bits ● 128 bits
Key Type ○ ASCII ● Hex
Characters Required
WEP Key

Remote Address
Bridge with Internal Network
WEP ○ Enabled ● Disabled
Key Length ○ 64 bits ● 128 bits
Key Type ○ ASCII ● Hex
Characters Required
WEP Key

The Wireless Distribution System (WDS) allows you to bridge wireless traffic between access points.

By wirelessly connecting APs to one another in an Extended Service Set, you can bridge distant Ethernets into a single LAN with each AP serving part of an area too large for a single AP to cover. WDS can extend the reach of your network into areas where cabling might be too difficult.

Caution:
Do not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges.

Loops created by WDS bridges with the intention of establishing backup links or extended service sets (ESS) with two WDS bridges on one AP will not work; they will result in endless loop data traffic on the network because Spanning Tree Protocol (STP) is not on the AP to prevent it.

More ...

Configuring WDS Settings

The following notes summarize critical guidelines regarding WDS configuration. Please read all the notes before proceeding with WDS configuration.

Notes

- When using WDS, be sure to configure WDS settings on *both* access points participating in the WDS link.
- You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.
- Both access points participating in a WDS link must be on the same radio channel and use the same IEEE 802.11 mode. (See “Radio” on page 129 for information on configuring the Radio mode and channel.)
- **Do not create loops** with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. *Spanning Tree Protocol* (STP), which manages path redundancy and prevent unwanted loops, is not available in the Professional Access Point. Keep these rules in mind when working with WDS on the access point:

  Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.

  Do not create backup links.

  If you can trace more than one path between any pair of APs going through any combination of Ethernet or WDS links, you have a loop.

  You can only extend or bridge either the Internal or Guest network but not both.

To configure WDS on this access point, describe each access point intended to receive hand-offs and send information to this access point. Each destination access point needs the following description:

Field	Description
Local Address	Indicates the Media Access Control (MAC) addresses for this access point. This is a read-only field.
Remote Address	Specify the MAC address of the destination access point; that is, the access point to which data will be sent and from which data will be received.
Bridge with	The Professional Access Point provides the capability of setting up guest and internal networks on the same access point. (See “Guest Login” on page 121.) The guest network typically provides internet access but isolates guest clients from more sensitive areas of your internal network. It is common to have security disabled on the guest network to provide open access. In contrast, the internal network provides full access to protected information behind a firewall and requires secure logins or certificates for access. When using WDS to link one access point to another, you need to identify the network within which you want the data exchange to occur. Specify the network to which you want to bridge this access point: • **Internal Network** • **Guest Network**

Field	Description
WEP	Specify whether you want Wired Equivalent Privacy (WEP) encryption enabled for the WDS link. • **Enabled** • **Disabled** Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. Both access points on the WDS link must be configured with the same security settings. For static WEP, a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.
Key Length	If WEP is enabled, specify the length of the WEP key: • **64 bits** • **128 bits**
Key Type	If WEP is enabled, specify the WEP key type: • **ASCII** • **Hex**
Characters Required	Indicates the number of characters required in the WEP key. The number of characters required updates automatically based on how you set key length and key type.
WEP Key	Enter a string of characters. • If you selected **ASCII** as your key type, enter any combination of `0-9`, `a-z`, and `A-Z`. • If you selected **HEX** as your key type, enter hexadecimal digits (any combination of `0-9` and `a-f` or `A-F`). These are the RC4 encryption keys shared with the stations using the access point.

Example of Configuring a WDS Link

When using WDS, be sure to configure WDS settings on both access points on the WDS link.

For example, to create a WDS link between the pair of access points `MyAP1` and `MyAP2` do the following:

1. Open the Web User Interface for MyAP1 by entering the IP address for MyAP1 as a URL in the Web browser address bar in the following form:

   ```
   http://IPAddressOfAccessPoint
   ```

   where *`IPAddressOfAccessPoint`* is the address of MyAP1.

2. Navigate to the WDS tab on MyAP1 Web User Interface.

The MAC address for MyAP1 (the access point you are currently viewing) will appear as the **Local Address** at the top of the page.

3. Configure a WDS interface for data exchange with MyAP2.

   Start by entering the MAC address for MyAP2 as the **Remote Address**, and fill in the rest of the fields to specify the network (guest or internal), security, and so on. Save the settings by clicking **Update**.

4. Navigate to the radio settings on the Web User Interface (Advanced menu's **Radio** tab) to verify or set the mode and the radio channel on which you want MyAP1 to broadcast.

   Remember that the two access points participating in the link, MyAP1 and MyAP2, must be set to the same mode and be transmitting on the same channel.

   For this example, suppose that you are using IEEE 802.11b mode and broadcasting on Channel 6. (Choose **Mode** and **Channel** from the drop-down lists on the Radio tab.)

5. Now repeat steps 1–4 for MyAP2:

   - Open the Web User Interface for MyAP2 by using MyAP2's IP address in a URL.

   - Navigate to the WDS tab on MyAP2 Web User Interface. MyAP2's MAC address will show as the **Local Address**.

   - Configure a WDS interface for data exchange with MyAP1, starting with the MAC address for MyAP1.

   - Navigate to the radio settings for MyAP2 to verify that it is using the same mode and broadcasting on the same channel as MyAP1. In this example, Mode is 802.11b and the channel is 6.

   - Be sure to save the settings by clicking **Update**.

Updating Settings

To apply your changes, click **Update**.

Time Protocol

The *Network Time Protocol* (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

The timestamp is used to indicate the date and time of each event in log messages.

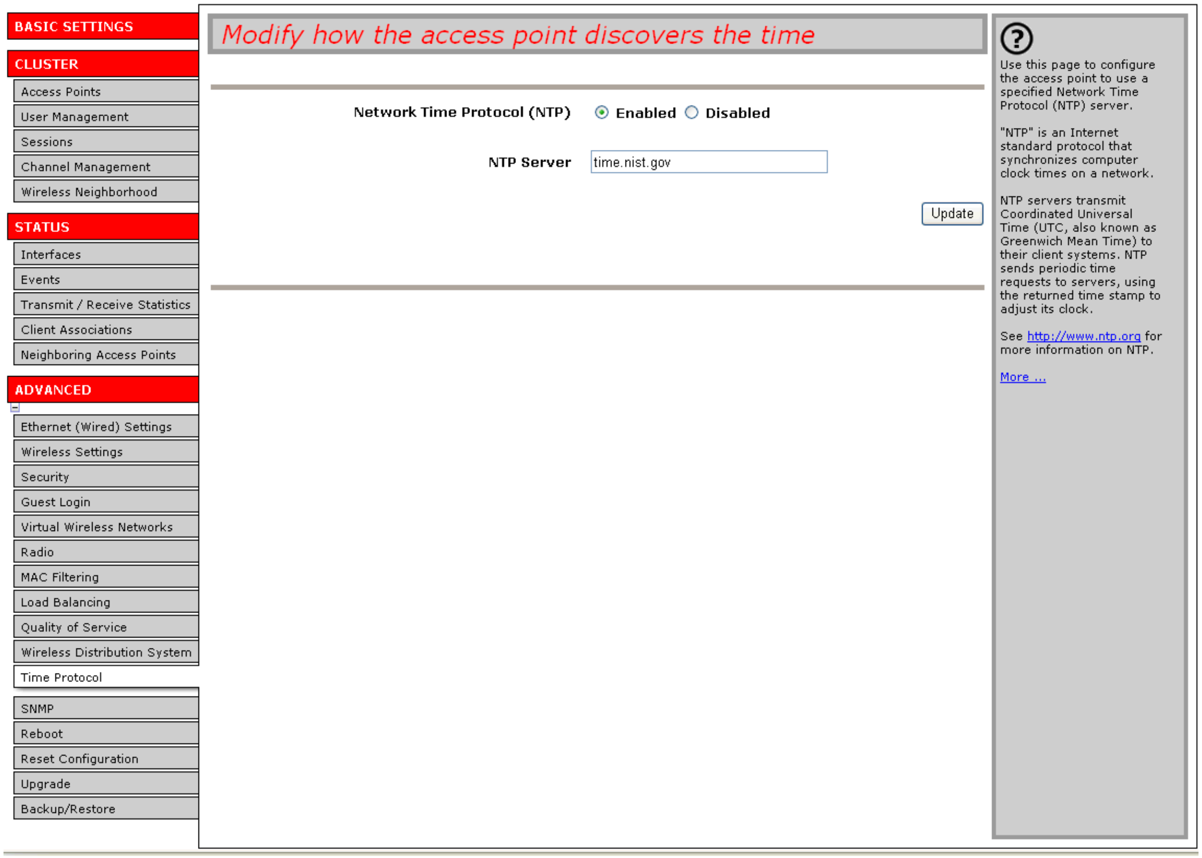
See http://www.ntp.org for more general information on NTP.

The following sections describe how to configure the Professional Access Point to use a specified NTP server:

- Navigating to Time Protocol Settings
- Enabling and Disabling a Network Time Protocol (NTP) Server
- Updating Settings

Navigating to Time Protocol Settings

To enable an NTP server, click the Advanced menu's **Time Protocol** tab, and update the fields as described below.



Modify how the access point discovers the time

Network Time Protocol (NTP) ● Enabled ○ Disabled

NTP Server: time.nist.gov

Use this page to configure the access point to use a specified Network Time Protocol (NTP) server.

"NTP" is an Internet standard protocol that synchronizes computer clock times on a network.

NTP servers transmit Coordinated Universal Time (UTC, also known as Greenwich Mean Time) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

See http://www.ntp.org for more information on NTP.

Enabling and Disabling a Network Time Protocol (NTP) Server

To configure your access point to use a network time protocol (NTP) server, first *enable* the use of NTP, and then select the NTP server you want to use. (To shut down NTP service on the network, disable NTP on the access point.

)

Field	Description
Network Time Protocol (NTP)	NTP provides a way for the access point to obtain and maintain its time from a server on the network. Using an NTP server gives your access point the ability to provide the correct time of day in log messages and session information. (See http://www.ntp.org for more general information on NTP.) Choose either to enable or to disable the use of a network time protocol (NTP) server: • **Enabled** • **Disabled**
NTP Server	If NTP is enabled, select the NTP server that you want to use. You can specify the NTP server by host name or IP address. However, using the host name is recommended because host names tend to be more constant than IP addresses.

Updating Settings

To apply your changes, click **Update**.

SNMP

The *Simple Network Management Protocol* (SNMP) is an Internet standard protocol that facilitates the monitoring and managing of network devices. SNMP lets you monitor events on your network through an SNMP software application.

The following sections describe how to configure SNMP on your network:

- Understanding SNMP
- Navigating to Simple Network Management Protocol
- Enabling and Disabling Simple Network Management Protocol (SNMP)
- Updating Settings
- Configuring Your Network Management System
- Rebooting and Upgrading Your Access Point Using SNMP

Understanding SNMP

SNMP defines a standard for recording, storing, and sharing information about network devices. SNMP is a subset of *Transmission Control Protocol/Internet Protocol* (TCP/IP) that facilitates network management, troubleshooting, and maintenance.

Key components of any SNMP-managed network are managed devices, SNMP agents, and a network management system. The agents, store data about their devices in *Management Information Bases* (MIBs) and return this data to the network management system when requested. Managed devices can be network nodes such as access point base stations, routers, switches, bridges, hubs, servers, or printers.

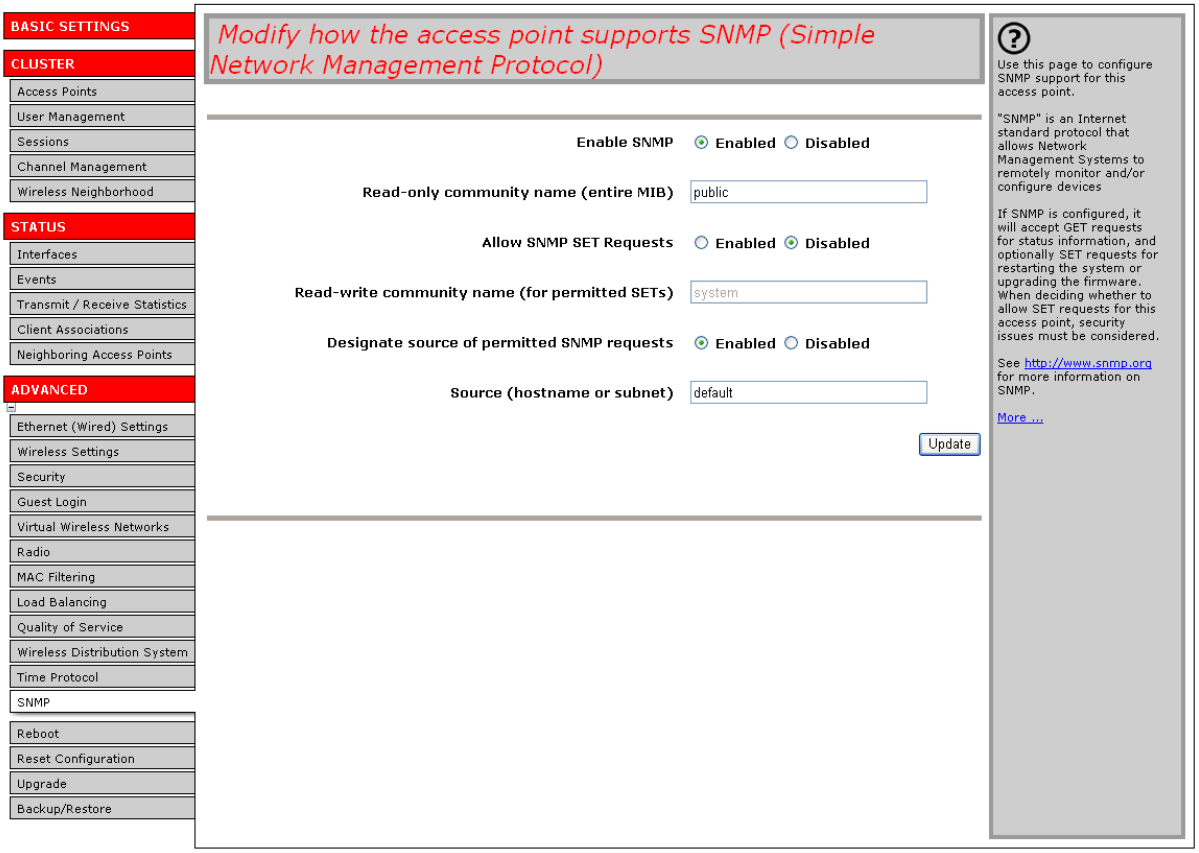
The Professional Access Point can function as an SNMP managed device for seamless integration into network management systems such as HP OpenView. The Professional Access Point supports the following SNMP MIBs:

- Standard SNMP MIBs
  - SNMP v1 and v2 MIBs
  - IEEE802.11 MIB
- Proprietary MIB
  - USR5453-PRODUCTS MIB—stores product identification information.
  - USR5453-SYSTEM MIB—facilitates system-level requests, such as reboot and upgrade.
  - USR5453-WIRELESS-CHAN MIB—maintains channel assignment information for access points in a cluster.
  - USR5453-WIRELESS-MIB—stores information about the wireless system, including peer statistics, beacon report, radio, and client statistics tables.

For more information about SNMP, visit http://www.snmplink.org.

Navigating to Simple Network Management Protocol

To enable SNMP, click the Advanced menu’s **SNMP** tab and update the fields as described below.



Modify how the access point supports SNMP (Simple Network Management Protocol)

Enable SNMP ● Enabled ○ Disabled

Read-only community name (entire MIB) public

Allow SNMP SET Requests ○ Enabled ● Disabled

Read-write community name (for permitted SETs) system

Designate source of permitted SNMP requests ● Enabled ○ Disabled

Source (hostname or subnet) default

Use this page to configure SNMP support for this access point.

"SNMP" is an Internet standard protocol that allows Network Management Systems to remotely monitor and/or configure devices

If SNMP is configured, it will accept GET requests for status information, and optionally SET requests for restarting the system or upgrading the firmware. When deciding whether to allow SET requests for this access point, security issues must be considered.

See http://www.snmp.org for more information on SNMP.

More ...

Enabling and Disabling Simple Network Management Protocol (SNMP)

To configure your access point to use Simple Network Management Protocol (SNMP) server, first *enable* the SNMP option that you want to use, and then provide the name of the community or host that can use the option.

Field	Description
Enable SNMP	SNMP provides a way for the access point to store management information and to provide the information to a network-management system (NMS). (See http://www.snmplink.org/ for more general information on SNMP.) Choose to either enable (default) or disable use of Simple Network Management Protocol:
Read-only Community Name (entire MIB)	If SNMP is enabled, enter the name of the community that is allowed to make information queries against the MIB. The community name acts an as authentication mechanism. The name functions as a password, and a request is considered authentic if the requester knows the password. The community name is alphanumeric; do not use special characters or spaces.
Allow SNMP SET Requests	Choose to either enable or disable the honouring of SNMP SET requests: • **Enable**—Machines on the network that provide the correct community name can issue SET requests. • **Disable**—(default) SET requests are not honoured. SET requests are restricted to the USR5453-SYSTEM MIB and USR5453-WIRELESS-CHAN MIB..
Read-write community name (for permitted SETs)	If SET requests are enabled, enter the name of the community that is allowed to make SET requests. The community name acts an as authentication mechanism. The name functions as a password, and a request is considered authentic if the requester knows the password. The community name is alphanumeric; do not use special characters or spaces.
Designate source of permitted SNMP requests	Choose to either enable or disable designating the source of the SNMP requests: • **Enable**—(default) A machine must be designated in the **Source** field in order for its requests to be honoured. • **Disable**—Any machine in the network may issue requests.

Field	Description
Source (hostname or subnet)	If source designation is enabled, enter the IP address of the host or subnet that is allowed to issue SNMP requests to the access point. If you use this option, the Professional Access Point honours requests from the specified host or subnet only. If you also enable a read-write community, the specified source must be a member of that community in order for the access point to honour the source's requests. **Note:** Even if you explicitly name a machine or a subnet in this field, any machine issuing a request must also know the proper community name in order to have the request honoured.

To shut down SNMP on the access point, select **Disable** in the **SNMP** field.

Updating Settings

To apply your changes, click **Update**.

Configuring Your Network Management System

In order to access the USRobotics proprietary MIBs, you need to import the MIBs into your network management system. You can find the MIB files in the Mib folder on the USRobotics CD-ROM. Refer to your network management system for instructions on importing and compiling MIBs.

Rebooting and Upgrading Your Access Point Using SNMP

In addition to the reboot and upgrade functions built into the Professional Access Points Web User Interface, you have the option of performing these functions through SNMP.

Rebooting Your Access Point Using SNMP.

Name	USR5453SystemReboot
Module	USR5453-SYSTEM-MIB
OID	1.3.6.1.4.1.9086.3.2.1
Base Syntax	OCTET STRING
Description	Setting this object to 1 will cause the access point to reboot.

Upgrading your Access Point

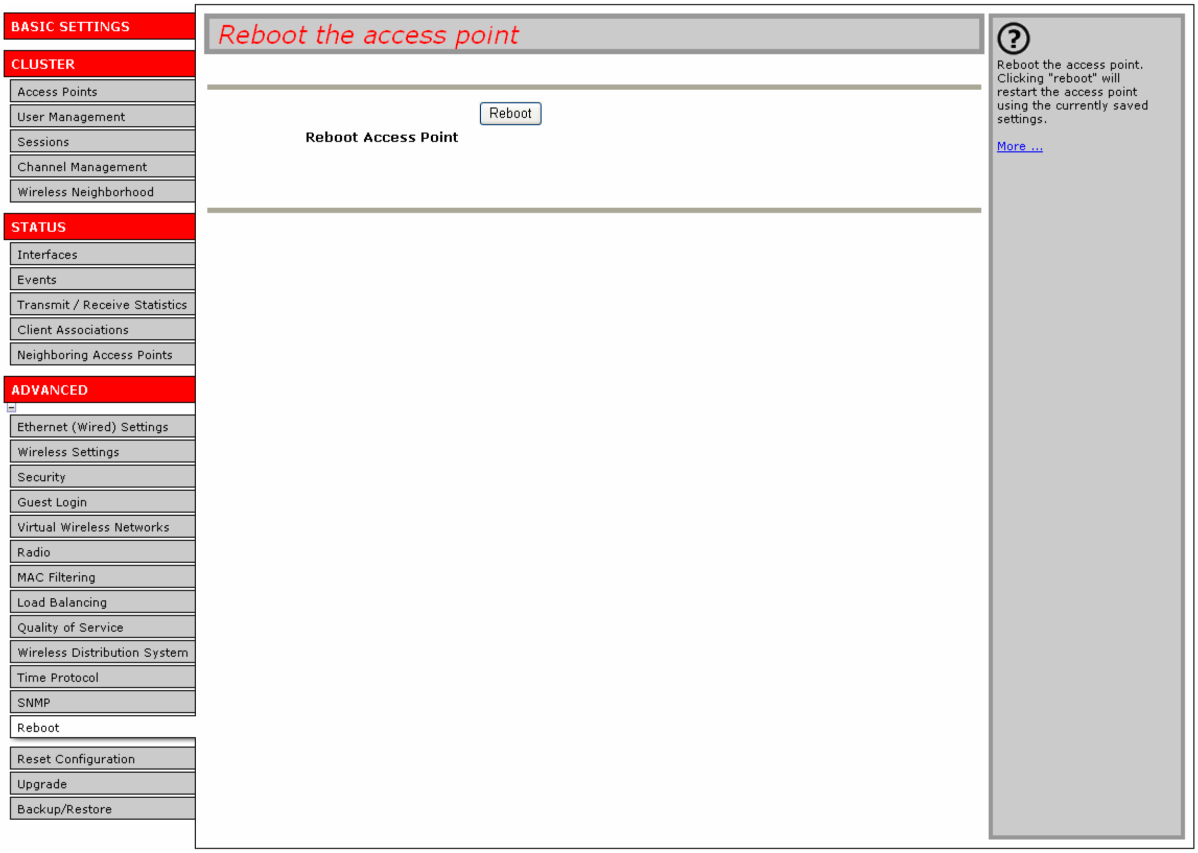
Name	USR5453SystemUpgrade
Module	USR5453-SYSTEM-MIB
OID	1.3.6.1.4.1.9086.3.2.2
Base Syntax	OCTET STRING

Description	Setting this object to a name of a file causes the device to download the file from the path specified. Set this object to an FTP or HTTP URL in order to upgrade the access point's firmware.
	FTP firmware upgrade:
	`ftp://username:password@IPaddress:FTPport/firmware-filename`
	By default *username* is `anonymous` and *FTPport* is `21`
	Examples:
	`ftp://testuser1:testuser1@192.168.1.99:22/5453_1.1.23.tar`
	`ftp://192.168.1.100/5453_1.1.24.tar`
	HTTP firmware upgrade:
	`http://IPaddress:HTTPport/firmware-filename`
	By default *HTTPport* is `80`
	Example:
	`http://192.168.1.101:8000/5453_1.1.24.tar`

Reboot

For maintenance purposes or as a troubleshooting measure, you can reboot the Professional Access Point as follows.

1. Click the Advanced menu's **Reboot** tab.



Reboot the access point. Clicking "reboot" will restart the access point using the currently saved settings.

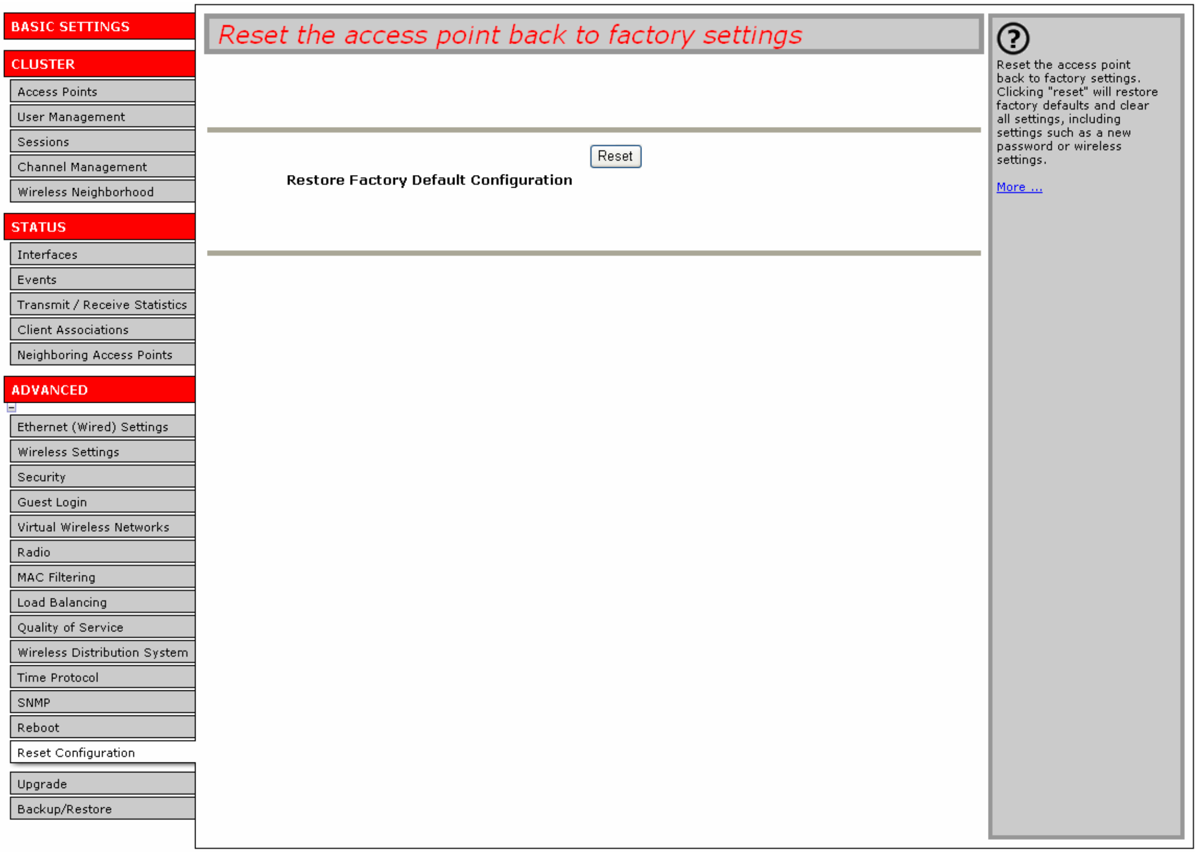
2. Click the **Reboot** button.

   The access point reboots. If the IP address of the access point changes after the reboot, you need to specify the new address in your Web browser in order to access the Web User Interface.

Reset Configuration

If you are experiencing extreme problems with the Professional Access Point and have tried all other troubleshooting measures, use the **Reset Configuration** function. This will restore factory defaults and clear all settings, including settings such as a new password and wireless settings.

1. Click the Advanced menu's **Reset Configuration** tab.



Reset the access point back to factory settings

Restore Factory Default Configuration

Reset the access point back to factory settings. Clicking "reset" will restore factory defaults and clear all settings, including settings such as a new password or wireless settings.

2. Click the **Reset** button.

   Factory defaults are restored.If the IP address of the access point changes after the reset, you need to specify the new address in your Web browser in order to access the Web User Interface.

Note Keep in mind that if you do reset the configuration from this page, you are doing so for this access point only; not for other access points in the cluster.

For information on the factory default settings, see “Default Settings for the Professional Access Point” on page 16.

If you cannot access the Web User Interface, you can reset the access point by using a thin object, such as a paper clip, to press the Reset button until both the LAN and WLAN LEDs turn off briefly.

Upgrade

As new versions of the Professional Access Point firmware become available, you can upgrade the firmware on your devices to take advantages of new features and enhancements.

Caution Do not upgrade the firmware from a wireless client that is associated with the access point you are upgrading. Doing so will cause the upgrade to fail. Furthermore, all wireless clients will be disassociated and no new associations will be allowed.

If you are reading this section because you already tried to upgrade the firmware through a wireless client, use a wired client to regain access to the access point as follows:

- Create a wired Ethernet connection from a PC to the access point.
- Open the Web User Interface.

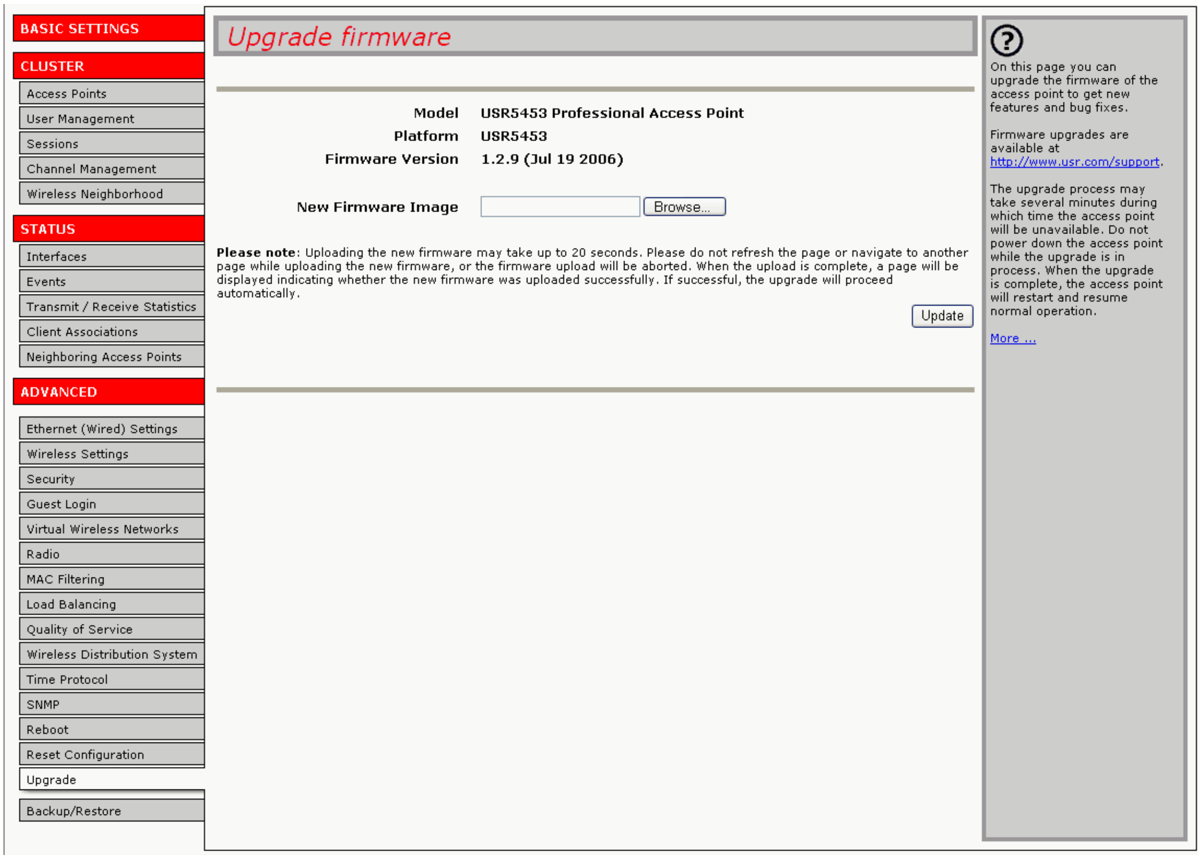
Repeat the upgrade process using with the wired client.

Caution The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point will restart and resume normal operation.

Note You must upgrade firmware for each access point; you cannot upgrade firmware automatically across the cluster.

To upgrade the firmware on a particular access point:

1. Navigate to Advanced menu's **Upgrade** tab on the Web User Interface for that access point.



Upgrade firmware

Model	USR5453 Professional Access Point
Platform	USR5453
Firmware Version	1.2.9 (Jul 19 2006)
New Firmware Image	

Please note: Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

On this page you can upgrade the firmware of the access point to get new features and bug fixes.

Firmware upgrades are available at http://www.usr.com/support.

The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point will restart and resume normal operation.

Information about the current firmware version is displayed and an option to upgrade a new firmware image is provided.

2. If you know the path to the **New Firmware Image** file, enter it in the textbox. Otherwise, click the **Browse** button and locate the firmware image file.

3. Click **Update** to apply the new firmware image.

   A confirmation window describes the upgrade process.

4. Click **OK** to confirm the upgrade and start the process.

Caution The firmware upgrade takes approximately 5 minutes, during which the Web User Interface displays a status message and progress bar. Do not power off the access point, and do not navigate away from the upgrade page in your Web browser during the firmware upgrade.

When the upgrade is complete, the Web User Interface redisplays the Upgrade firmware page. You can verify that the ugrade was successful by checking the firmware version shown on that page.

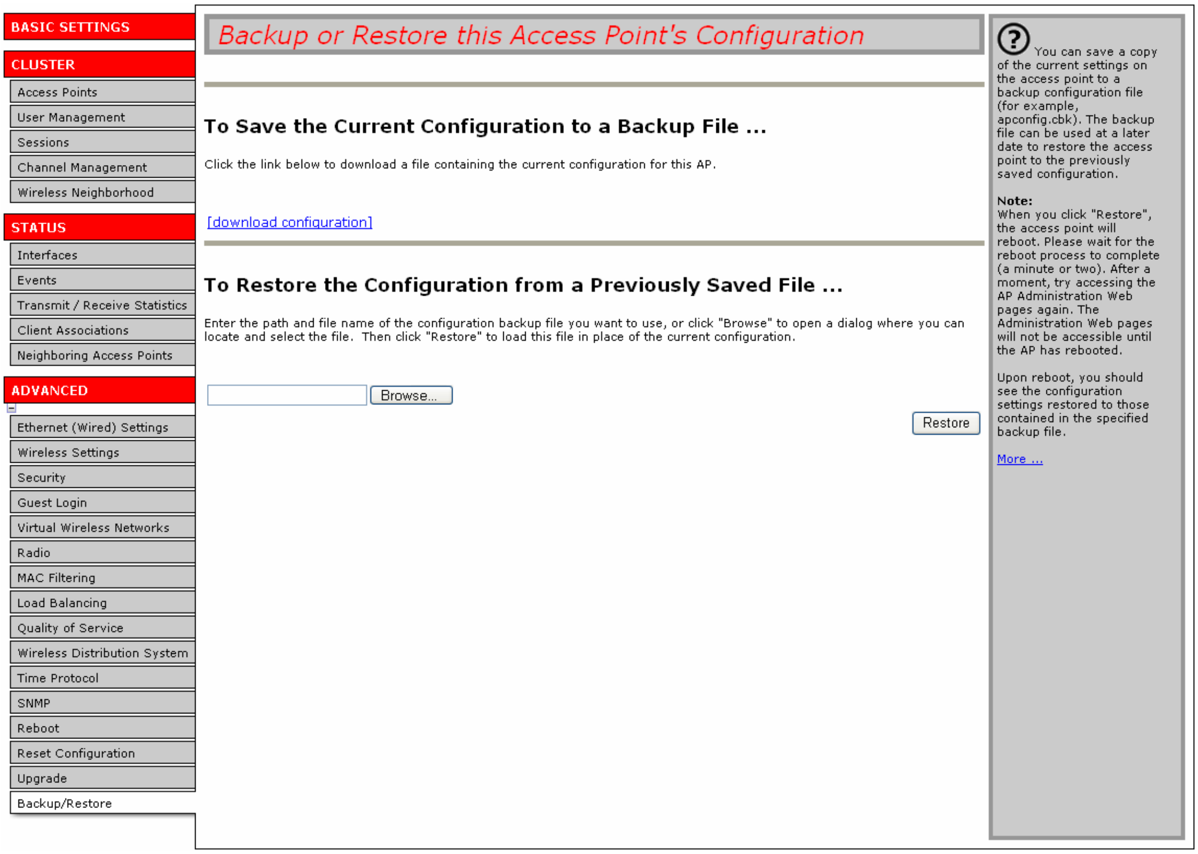
Backup/Restore

You can save a copy of the current settings on the Professional Access Point to a backup configuration file. The backup file can be used at a later date to restore the access point to the previously saved configuration.

- Navigating to Backup and Restore Settings
- Backing up Configuration Setting for an Access Point
- Restoring Access Point Settings to a Previous Configuration

Navigating to Backup and Restore Settings

To backup or restore a configuration for an access point, click the Advanced menu’s **Backup and Restore** tab and use the Web User Interface as described below.



Backup or Restore this Access Point's Configuration

To Save the Current Configuration to a Backup File ...

Click the link below to download a file containing the current configuration for this AP.

[download configuration]

To Restore the Configuration from a Previously Saved File ...

Enter the path and file name of the configuration backup file you want to use, or click "Browse" to open a dialog where you can locate and select the file. Then click "Restore" to load this file in place of the current configuration.

You can save a copy of the current settings on the access point to a backup configuration file (for example, apconfig.cbk). The backup file can be used at a later date to restore the access point to the previously saved configuration.

Note:
When you click "Restore", the access point will reboot. Please wait for the reboot process to complete (a minute or two). After a moment, try accessing the AP Administration Web pages again. The Administration Web pages will not be accessible until the AP has rebooted.

Upon reboot, you should see the configuration settings restored to those contained in the specified backup file.

More ...

Backing up Configuration Setting for an Access Point

To save a copy of the current settings on an access point to a backup configuration file (`.cbk` format):

1. Click the **download configuration** link.

   A File Download or Open dialogue is displayed.

2. Choose the **Save** option on this first dialogue.

   This brings up a file browser.

3. Use the file browser to navigate to the directory where you want to save the file, and click **Save** to save the file.

   You can use the default file name (`apconfig.cbk`) or type a new name for the backup file, but be sure to save the file with a `.cbk` extension.

Restoring Access Point Settings to a Previous Configuration

To restore the configuration on an access point to previously saved settings:

1. Select the backup configuration file you want to use, either by typing the full path and file name in the Restore field or by clicking **Browse**, selecting the file, and clicking **Open**.

   (Only those files that were created with the Backup function and saved as `.cbk` backup configuration files are valid to use with **Restore**; for example, `apconfig.cbk`.)

2. Click the **Restore** button.

   The access point will reboot.

   Note When you click **Restore**, the access point will reboot. A reboot confirmation dialogue and follow-on rebooting status message will be displayed. Wait a minute or two for the reboot process to complete. Then try to access the Web User Interface as described in the next step; the Web User Interface will not be accessible until the access point has rebooted.

3. When the access point has rebooted, access the Web User Interface either by clicking again on one of the tabs (if the Web User Interface is still displayed) or by typing the IP address the Professional Access Point as a URL in the address field of the Web browser. Enter the URL for the access point as `http://`*`IPAddressOfAccessPoint`*.

   The Web User Interface displays the configuration settings restored from the backup file that you selected.

Command Line Interface

In addition to the Web-based user interface, the Professional Access Point includes a command line interface (CLI) for administering the access point. The CLI lets you view and modify status and configuration information.

From the client station perspective, even a single deployed Professional Access Point broadcasting its "network name" to clients constitutes a *wireless network*. Keep in mind that CLI configuration commands, like Web User Interface settings, can affect a single access point running in stand-alone mode or automatically propagate to a network of *clustered* access points that share the same settings. (For more information on clustering, see “Access Points” on page 43. For information on how to set an access point to stand-alone or cluster mode from the CLI, see “Set Configuration Policy for New Access Points” on page 39)

This part of the Professional Access Point Administrator Guide introduces the interface and provides a complete description of classes and their associated fields:

- Class Structure, Commands, and Examples
- Class and Field Reference

Class Structure, Commands, and Examples

The following topics in this appendix provide an introduction to the class structure upon which the CLI is based, CLI commands, and examples of using the CLI to get or set configuration information on an access point or cluster of APs:

- Comparison of Settings Configurable with the CLI and Web User Interface
- How to Access the CLI for an Access Point
  - Telnet Connection to the Access Point
  - SSH2 Connection to the Access Point
- Quick View of Commands and How to Get Help
- Command Usage and Configuration Examples
  - Understanding Interfaces as Presented in the CLI
  - Saving Configuration Changes
  - Basic Settings

Comparison of Settings Configurable with the CLI and Web User Interface

The command line interface (CLI) and the Web User Interface to the Professional Access Point are designed to suit the preferences and requirements for different types of users or scenarios. Most administrators will probably use both interfaces in different contexts. Some features (such as Clustering) can only be configured from the Web User Interface, and some details and more complex configurations are only available through the CLI.

The CLI is particularly useful in that it provides an interface to which you can write programmatic scripts for access point configurations. Also, the CLI may be less resource-intensive than a Web interface.

The following table shows a feature-by-feature comparison of which settings can be configured through the CLI or the Web User Interface, and which are configurable with either.

Feature or Setting	Configurable from CLI	Configurable from Web User Interface
Basic Settings • Getting/changing Administrator Password • Getting/changing access point name and location • Viewing information like MAC, IP address, and Firmware version	yes	yes
Access Point and Cluster Settings	Get existing settings only. You cannot set configuration *policy* or other cluster features from the CLI. Use for clustering settings.	yes
User Accounts	yes	yes
User Database Backup and Restore	You cannot backup or restore a user database from the CLI. To restore a user database, use the Web User Interface as described in "Backing Up and Restoring a User Database" on page 56.	yes
Sessions	The CLI does not provide session monitoring information. To view client sessions, use the Web User Interface.	yes
Channel Management	You cannot configure Channel Management from the CLI. To configure channel management, use the Web User Interface as described in "Channel Management" on page 63.	yes
Wireless Neighborhood	You cannot view the cluster-based "Wireless Neighborhood" from the CLI. To view the wireless neighbourhood,use the Web User Interface as described in "Wireless Neighborhood" on page 71.	yes
Status	yes	yes

Feature or Setting	Configurable from CLI	Configurable from Web User Interface
Ethernet (Wired) Interface	**yes** You can configure all Ethernet (Wired) settings from the CLI except "Connection Type". To change the Connection Type from DHCP to Static IP addressing (or vice versa), you must use the Web User Interface.	**yes**
Wireless Interface	**yes**	**yes**
Security	**yes**	**yes**
Set Up Guest Access	**yes**	**yes**
Enable/Configure Guest Login Welcome Page	**yes**	
Configuring Multiple BSSIDs on Virtual Wireless Networks	**yes**	**yes**
Radio Settings	**yes** You can configure all Radio settings from the CLI except for turning on/off Super G.	**yes**
MAC Filtering	**yes**	**yes**
Load Balancing	**yes**	**yes**
Quality of Service	**yes**	**yes**
Wireless Distribution System	**yes**	**yes**
Time Protocol	**yes**	**yes**
Reboot the Access Point	**yes**	
Reset the Access Point to Factory Defaults	**yes**	**yes**
Upgrade the Firmware	You cannot upgrade the firmware from the CLI. To upgrade firmware, use the Web User Interface as described in "Upgrade" on page 172.	**yes**
Backup and Restore	You cannot backup or restore an access point configuration from the CLI. To backup or restore an access point configuration, use the Web User Interface as described in "Backup/Restore" on page 174.	**yes**

How to Access the CLI for an Access Point

Use one of the following methods to access the command line interface (CLI) for the access point or wireless network:

- Telnet Connection to the Access Point
- SSH2 Connection to the Access Point

Telnet Connection to the Access Point

If you already have your network deployed and know the IP address of your access point, you can use a remote Telnet connection to the access point to view the system console over the network.

Note The default Static IP address is 192.168.1.10. If there is no DHCP server on the network, the access point retains this static IP address at first-time startup. You can use the Detection Utility to find the IP address of the access point. (For more about IP addressing, see “Understanding Dynamic and Static IP Addressing on the Professional Access Point” on page 20)

1. Bring up a command window on your PC.

   (For example, from the Start menu, select **Run** to bring up the Run dialogue, type `cmd` in the Open field, and click **OK**.)

2. At the command prompt, type the following:

   ```
   telnet IPAddressOfAccessPoint
   ```

   where *`IPAddressOfAccessPoint`* is the address of the access point you want to monitor.

   (If your Domain Name Server is configured to map domain names to IP addresses via DHCP, you can also telnet to the domain name of the access point.)

3. You will be prompted for an Administrator user name and password for the access point.

   ```
   USR5453-AP login:
   Password:
   ```

   Enter the default Administrator username and password for the Professional Access Point (`admin`, `admin`), and press "Enter" after each. (The password is masked, so it will not be displayed on the screen.)

   When the user name and password is accepted, the screen displays the Professional Access Point help command prompt.

   ```
   USR5453-AP login: admin
   Password:
   Enter 'help' for help.
   ```

You are now ready to enter CLI commands at the command line prompt. In addition to commands that affect the behavior or the access point, the CLI supports the following commands that pertain to Telnet status:

Telnet Function	Telnet Command
Get the current Telnet status	`get telnet status`
Enable Telnet acess	`set telnet status up`
Disable Telnet access	`set telnet status down`
Generate a new pair of SSH keys	`set ssh gen-key yes` **Note:** This command may take up to 2 minutes to complete.After issuing this command, you must reboot the AP for the new keys to take effect.

Notes Any change that you make to the access point configuration through the command line interface remains in effect for the current session. To save your changes across sessions, use the save-running command

SSH2 Connection to the Access Point

If you already have your network deployed and know the IP address of your access point, you can use a remote SSH2 connection to the access point to view the system console over the network.

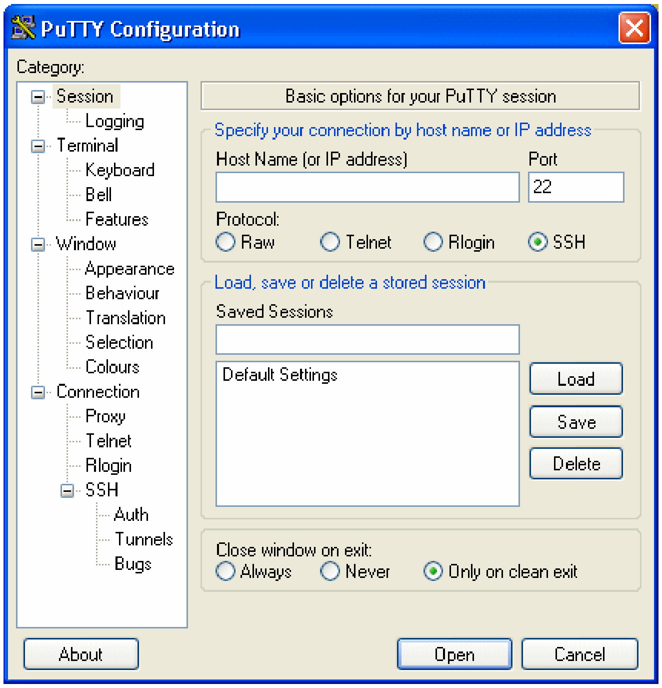
Notes The Professional Access Point supports SSH version 2 only.

The default Static IP address is 192.168.1.10. If there is no DHCP server on the network, the access point retains this static IP address at first-time startup. You can use the Detection Utility to find the IP address of the access point. (For more about IP addressing, see "Understanding Dynamic and Static IP Addressing on the Professional Access Point" on page 20.)

Using an SSH2 connection to the access point is similar to Telnet in that it gives you remote access to the system console and CLI. SSH2 has the added advantage of being a secure connection traffic encrypted.

To use an SSH2 connection, you need to have SSH software installed on your PC (such as PuTTY, which is available at http://www.chiark.greenend.org.uk/~sgtatham/putty/).

1. Start your SSH application. (This example uses PuTTY.)



Host Name (or IP address):
Port: 22
Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH
Close window on exit: ○ Always ○ Never ● Only on clean exit

2. Enter the IP address of the access point and click **Open**.

   (If your Domain Name Server is configured to map domain names to IP addresses via DHCP, you can enter the domain name of the access point instead of an IP address.)

   This brings up the SSH command window and establishes a connection to the access point. The login prompt is displayed.

   ```
   login as:
   ```

3. Enter the default Administrator username and password for the Professional Access Point (`admin`, `admin`), and press "Enter" after each. (The password is masked, so it will not be displayed on the screen.)

   ```
   login as: admin
   admin@10.10.100.110's password:
   Enter 'help' for help.
   ```

   When the user name and password is accepted, the screen displays the Professional Access Point help command prompt.

   ```
   USR5453-AP#
   ```

You are now ready to enter CLI commands at the command line prompt. In addition to commands that affect the behavior or the access point, the CLI supports the following commands that pertain to Telnet status:

SSH Function	SSH Command
Get the current SSH status	`get ssh status`
Enable SSH acess	`set ssh status up`
Disable SSH access	`set ssh status down`

Notes Any change that you make to the access point configuration through the command line interface remains in effect for the current session. To save your changes across sessions, use the save-running command

Quick View of Commands and How to Get Help

- Commands and Syntax
- Getting Help on Commands at the CLI
- Ready to Get Started?

Caution Settings updated from the CLI (with **get**, **set**, **add**, **remove** commands) will not be saved to the startup configuration unless you explicitly save them via the **save-running** command. For a description of configurations maintained on the access point and details on how to save your updates, see "“Saving Configuration Changes” on page 191.

Commands and Syntax

The CLI for the Professional Access Point provides the following commands for manipulating objects.

Notes

- `named_class` is a class of an object from the configuration whose instances are individually named.
- `instance` is a name of an instance of class.
- field values cannot contain spaces unless the value is in quotes

For a detailed class and field reference, see “Class and Field Reference” on page 253.

Command	Description
get	The "get" command allows you to get the field values of existing instances of a class. Classes can be "named" or "unnamed". The command syntax is: **get** *unnamed-class* [*field* ... | **detail**] **get** *named-class* [*instance* | **all** [*field* ... | *name* | **detail**]] The rest of the command line is optional. If provided, it is either a list of one or more *`fields`*, or the keyword **detail**. An example of using the "get" command on an unnamed class with a single instance is: **`get log`** (There is only one log on the access point. This command returns information on the log file.) An example of using the "get" command on an unnamed class with multiple instances is: **`get log-entry`** (There are multiple log entries but they are not named. This command returns all log entries.) An example of using the "get" command on a named class with multiple instances is: **`get bss wlan0bssInternal`** (There are multiple bss's and they are named. This command returns information on the BSS named "wlan0bssInternal".) An example of using the "get" command on a named class to get all instances: **`get radius-user all name`** **`get radius-user all`** **Note:** "`wlan0bssInternal`" is the name of the basic service set (BSS) on the internal network (`wlan0` interface). For information on *interfaces*, see "Understanding Interfaces as Presented in the CLI" on page 190.

Command	Description
set	The "set" command allows you to set the field values of existing instances of a class. **set** *unnamed-class* [**with** *qualifier-field qualifier-value* ... **to**] *field value . . .* The first argument is an unnamed class in the configuration. After this is an optional qualifier that restricts the set to only some instances. For singleton classes (with only one instance) no qualifier is needed. If there is a qualifier, it starts with the keyword **with**, then has a sequence of one or more *qualifier-field qualifier-value* pairs, and ends with the keyword **to**. If these are included, then only instances whose present value of *qualifier-field* is *qualifier-value* will be set. The *qualifier-value* arguments cannot contain spaces. Therefore, you cannot select instances whose desired *qualifier-value* has a space in it. The rest of the command line contains *field-value* pairs. **set** *named-class instance* | **all** [with *qualifier-field qualifier-value* ... **to**] *field value . . .* The first argument is either a named class in the configuration. The next argument is the name of the *instance* to set, or the keyword **all**, which indicates that all instances should be set. Classes with multiple instances can be set consecutively in the same command line as shown in Example 4 below. The *qualifier-value* arguments cannot contain spaces. Here are some examples. (Bold text indicates class names, field names, or keywords; text that is not bold indicates values to which the fields are being set.) 1. **set interface wlan0 ssid** "Vicky's AP" 2. **set radio all beacon-interval** 200 3. **set tx-queue wlan0 with queue data0 to aifs** 3 4. **set tx-queue wlan0 with queue data0 to aifs** 7 **cwmin** 15 **cwmax** 1024 **burst** 0 5. **set bridge-port br0 with interface eth0 to path-cost** 200 **Note:** For information on *interfaces* used in this example (such as wlan0, br0, or eth0) see “Understanding Interfaces as Presented in the CLI” on page 190.
add	The "add" command allows you to add a new instance of a class. **add** *named-class instance* [*field value* ...] **add** *anonymous-class* [*field value* ...] For example: **add radius-user** wally

Command	Description
remove	The "remove" command allows you to remove an existing instance of a class. **remove** *unnamed-class* [*field value* . . .] **remove** *named-class instance* | **all** [*field value* . . .] For example: `remove radius-user wally`

The CLI also includes the following commands for maintenance tasks:

save-running	The **save-running** command saves the running configuration as the startup configuration. For more information, see ““Saving Configuration Changes” on page 191.
reboot	The **reboot** command restarts the access point (a soft reboot). For more information, see ““Reboot the Access Point” on page 247.
factory-reset	The **factory-reset** command resets the access point to factory defaults and reboots. For more information, see ““Reset the Access Point to Factory Defaults” on page 247.

Getting Help on Commands at the CLI

Help on commands can be requested at the command line interface (CLI) by using the TAB key. This is a quick way to see all valid completions for a class.

Hitting TAB once will attempt to complete the current command.

If multiple completions exist, a beep will sound and no results will be displayed. Enter TAB again to display all available completions.

- **Example 1:** At a blank command line, hit TAB twice to get a list of all commands.

```
USR5453-AP#
add             Add an instance to the running configuration
factory-reset   Reset the system to factory defaults
get             Get field values of the running configuration
reboot          Reboot the system
remove          Remove instances in the running configuration
save-running    Save the running configuration
set             Set field values of the running configuration
```

- **Example 2:** Type "**get** " TAB TAB (including a space after **get**) to see a list of all field options for the **get** command.

```
USR5453-AP# get
association      Associated station
basic-rate       Basic rate of the radio
bridge-port      Bridge ports of bridge interfaces
bss              Basic Service Set of the radio
```

```
cluster           Clustering-based configuration settings
cluster-member    Member of a cluster of like-configured access points
config            Configuration settings
detected-ap       Detected access point
dhcp-client       DHCP client settings
dot11             IEEE 802.11
host              Internet host settings
interface         Network interface
ip-route          IP route entry
klog-entry        Kernel log entry
log               Log settings
log-entry         Log entry
mac-acl           MAC address access list item
ntp               Network Time Protocol client
portal            Guest captive portal
radio             Radio
radius-user       RADIUS user
ssh               SSH access to the command line interface
supported-rate    Supported rate of the radio
system            System settings
telnet            Telnet access to the command line interface
tx-queue          Transmission queue parameters
wme-queue         Transmission queue parameters for stations
```

- **Example 3:** Type "**get system v**" TAB. This will result in completion with the only matching field, "**get system version**". Hit ENTER to display the output results of the command.

For detailed examples on getting help, see “Tab Completion and Help” on page 248.

Ready to Get Started?

If you know the four basic commands shown above (**get**, **set**, **remove**, and **add**) and how to get help at the CLI using tab completion, you are ready to get started.

The best way to get up-to-speed quickly is to bring up the CLI on your access point and follow along with some or all of the examples in the next topic “Command Usage and Configuration Examples” on page 188.

Command Usage and Configuration Examples

“Understanding Interfaces as Presented in the CLI” on page 190

“Saving Configuration Changes” on page 191

“Basic Settings” on page 192

“Access Point and Cluster Settings” on page 196

“User Accounts” on page 196

“Status” on page 199

"Ethernet (Wired) Interface" on page 207

"Wireless Interface" on page 213

"Security" on page 213

"Enable/Configure Guest Login Welcome Page" on page 228

"Configuring Multiple BSSIDs on Virtual Wireless Networks" on page 229

"Radio Settings" on page 230

"MAC Filtering" on page 235

"Load Balancing" on page 238

"Quality of Service" on page 238

"Wireless Distribution System" on page 245

"Time Protocol" on page 246

"Reboot the Access Point" on page 247

"Reset the Access Point to Factory Defaults" on page 247

"Keyboard Shortcuts" on page 248

Understanding Interfaces as Presented in the CLI

The following summary of interface names is provided to help clarify the related CLI commands and output results. These names are not exposed on the Web User Interface, but are used throughout the CLI. You get and set many configuration values on the access point by referring to interfaces. In order to configure the access point through the CLI, you need to understand which interfaces are available on the access point, what role they play (corresponding setting on the Web User Interface), and how to refer to them.

Interface	Description
lo	Local loopback for data meant for the access point itself.
eth0	The wired (Ethernet) interface for the Internal network.
br0	The Internal bridge represents the Internal interface for the access point. To telnet or ssh into the access point, use the IP address for this interface. br0 consists: • eth0 (or vlan`SomeNumber` if you have VLANs configured) • wlan0 The IP address of the access point is provided in the output detail for br0. So, a useful command is **get interface**. This gives you common information on all interfaces. From the output results, you can find the IP address for `br0`. Use this IP address to connect to the access point.
brguest	The Guest bridge, which consists of eth1 and wlan0guest.
brvwn1	The bridge interface for Virtual Wireless Network (VWN) 1. The bridge interface for VWN1 consists of: • `wlan0vwn1` • `vlanVLANID` where `VLANID` is a four-digit VLAN ID that you provided. (For example, if you provided a VLAN ID of 1234, the VLAN interface would be "`vlan1234`"
brvwn2	This is for the second Virtual Wireless Network (VWN) 2. The bridge interface for VWN2 consists of: • `wlan0vwn1` • `vlanVLANID` where `VLANID` is a four-digit VLAN ID that you provided. (For example, if you provided a VLAN ID of 1234, the VLAN interface would be `vlan1234`.)
wlan0	The wireless (radio) interface for the Internal network.
wlan0guest	The wireless (radio) interface for the Guest network.
wlan0vwn1	The wireless interface for Virtual Wireless Network (VWN) 1.
wlan0vwn2	The wireless interface for Virtual Wireless Network (VWN) 2.

Interface	Description
wlan0wds*x*	A wireless distribution system (WDS) interface where "x" indicates the number of the WDS link. (For example, `wlan0wds1`.)

vlanxxxx	A VLAN interface for VLAN ID `xxxx`. To find out what this VLAN interface is (Internal, Guest, VWN1 or VWN2), use the following command to look at the "`role`" field:
	`get interface vlanVLANID role`
	For example:
	`get interface vlan1234 role`

Saving Configuration Changes

The Professional Access Point maintains three different configurations.

- **Factory Default Configuration** - This configuration consists of the default settings shipped with the access point (as specified in "Default Settings for the Professional Access Point" on page 16).

  You can always return the access point to the factory defaults by using the **factory-reset** command, as described in "Reset the Access Point to Factory Defaults" on page 247.

- **Startup Configuration** - The startup configuration contains the settings that the access point will use the next time it starts up (for example, upon reboot).

  To save configuration updates made from the CLI to the *startup* configuration, you must execute the **save-running** or "**set config startup running**" command from the CLI after making changes.

- **Running Configuration** - The running configuration contains the settings with which the access point is currently running.

  When you view or update configuration settings through the command line interface (CLI) using **get**, **set**, **add**, and **remove** commands, you are viewing and changing values on the *running* configuration only. If you do not save the configuration (by executing the **save-running** or "**set config startup running**" command at the CLI), you will lose any changes you submitted via the CLI upon reboot.

The **save-running** command saves the *running* configuration as the startup configuration. (The **save-running** command is a shortcut command for "**set config startup running**", which accomplishes the same thing)

Settings updated from the CLI (with **get**, **set**, **add**, **remove** commands) will not be saved to the startup configuration unless you explicitly save them via the **save-running** command. This gives you the option of maintaining the *startup* configuration and trying out values on the *running* configuration that you can discard (by not saving).

By contrast, configuration changes made from the Web User Interface are automatically saved to both the *running* and *startup* configurations. If you make changes from the Web User Interface that you do not want to keep, your only option is to reset to factory defaults. The previous startup configuration will be lost.

Basic Settings

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 190. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, or to the Internal or Guest network.

The following CLI command examples correspond to tasks you can accomplish on the Basic Settings tab of the Web User Interface for access points with clustering capabilities. In some cases, the CLI **get** command provides additional details not available through the Web User Interface.

This table shows a quick view of Basic Settings commands and provides links to detailed examples.

Basic Setting	Example

Get the IP Address for the Internal Interface on an Access Point	`get interface br0 ip`
	or
	`get interface`
	get interface is a catch-all command that shows common information on all interfaces for the access point such as IP addresses, MAC addresses, and so on. The IP address for the Internal interface (and the one used to access the access point) is that shown for br0. (See "Understanding Interfaces as Presented in the CLI" on page 190)

Get the MAC Address for an Access Point	`get interface br0 mac`
Get Both the IP Address and MAC Address	`get interface br0 mac ip`
Get Common Information on All Interfaces for an Access Point	`get interface`
Get the Firmware Version for the Access Point	`get system version`
Get the Location of the Access Point	`get cluster location`

Set the Location for an Access Point	`set system location` *`NewLocation`*
	For example:
	`set system location hallway`
	or
	`set system location "Vicky's Office"`

Get the Current Password	`get system encrypted-password`

Set the Password	`set system password` *`NewPassword`*
	For example:
	`set system password admin`

Get the Wireless Network Name (SSID))	`get interface wlan0 ssid`

Basic Setting	Example

Set the Wireless Network Name (SSID)	`set interface wlan0 ssid` *`NewSSiD`*
	
	For example:
	`set interface wlan0 ssid Vicky`
	`set interface wlan0 ssid "Vicky's AP"`

Get the IP Address for the Internal Interface on an Access Point

In the following example, the IP address for the access point is: 10.10.55.216. Use the **get** command as shown to obtain the IP address for the Internal network.

```
USR5453-AP# get interface br0 ip
10.10.55.216
```

Get the MAC Address for an Access Point

In the following example, the MAC address for the access point is: 00:a0:c9:8c:c4:7e. Use the **get** command as shown to obtain the MAC address.

```
USR5453-AP# get interface br0 mac
00:a0:c9:8c:c4:7e
```

Get Both the IP Address and MAC Address

The following command returns both the IP address and the MAC address for an access point:

```
USR5453-AP# get interface br0 mac ip
Field  Value
---------------------
ip     10.10.55.216
mac    00:a0:c9:8c:c4:7e
```

Get Common Information on All Interfaces for an Access Point

The following example shows common information (including IP addresses) for all interfaces.

```
USR5453-AP# get interface
name        type         status  mac                ip             mask
---------------------------------------------------------------------------
-----
lo                      up      00:00:00:00:00:00  127.0.0.1      255.0.0.0
eth0                     up      00:02:B3:01:01:01
eth1                     down    00:02:B3:02:02:02
br0         bridge       up      00:02:B3:01:01:01  10.10.100.110
255.255.255.0
brguest     bridge       down    00:00:00:00:00:00
wlan0       service-set  up      00:0C:41:16:DF:A6
wlan0guest  service-set  up
wlan0wds0   wds          down
```

```
wlan0wds1   wds          down
wlan0wds2   wds          down
wlan0wds3   wds          down
USR5453-AP#
```

Get the Firmware Version for the Access Point

In the following example, the access point is running Firmware Version: 1.0.0.9. Use the **get** command as shown to obtain the Firmware Version.

```
USR5453-AP# get system version
1.0.0.9
```

Get the Location of the Access Point

In the following example, the location of the access point has not been set. Use the **get** command as shown to obtain the location of the access point.

```
USR5453-AP# get cluster location
not set
```

Set the Location for an Access Point

To set the location for an access point, use the **set** command as follows:

```
USR5453-AP# set system location hallway
USR5453-AP# set system location "Vicky's Office"
```

To check to make sure that the location was set properly, use the **get** command again to find out the location

```
USR5453-AP# get system location
Vicky’s Office
```

Get the Current Password

```
USR5453-AP# get system encrypted-password
2yn.4fvaTgedM
```

Set the Password

```
USR5453-AP# set system password admin
USR5453-AP# get system encrypted-password
/rYSvxS4Okptc
```

Get the Wireless Network Name (SSID)

```
USR5453-AP# get interface wlan0 ssid
Internal Instant802 Network
```

Set the Wireless Network Name (SSID)

```
USR5453-AP# set interface wlan0 ssid "Vicky’s AP"
USR5453-AP# get interface wlan0 ssid
Vicky’s AP
```

Access Point and Cluster Settings

The command examples in this section show how to get the configuration for a cluster of access points. These settings generally correspond to those on the Cluster menu's Access Points tab in the Web User Interface.

Note You cannot use the CLI to add or remove an access point from a cluster or set the configuration policy. If you want to configure clustering, please use the Web User Interface as described in "Access Points" on page 43

This table provides a quick view of Access Point Cluster commands and provides links to detailed examples.

Cluster Command	Example
Determine whether the Access Point is a Cluster Member or is in Stand-alone Mode	`get cluster detail`
Get MAC Addresses for all Access Points in the Cluster	`get clustered-ap all name`

Determine whether the Access Point is a Cluster Member or is in Stand-alone Mode

This command shows whether the access point is clustered or not. If the command returns 0, the access point is in stand-alone mode (not clustered). If the command returns 1, the access point is a member of a cluster. In the following example, the access point is in stand-alone mode.

```
USR5453-AP# get cluster detail
Field         Value
--------------------
clustered     0
clusterable   0
kickstarted   0
location      not set
formation
```

Get MAC Addresses for all Access Points in the Cluster

```
USR5453-AP# get cluster-member all
name                mac                 ip            location  removed
---------------------------------------------------------------------
00:e0:b8:76:23:b4   00:e0:b8:76:23:b4   10.10.10.248  not set   0
00:e0:b8:76:16:88   00:e0:b8:76:16:88   10.10.10.230  not set   0
```

User Accounts

The following command examples show configuration tasks related to user accounts. These tasks correspond to the Cluster menu's User Management tab in the Web User Interface.

This table shows a quick view of User Management commands and provides links to detailed examples.

User Account Command	Example

Get All User Accounts	To view all usernames:
	`get radius-user all name`
	To view all user accounts:
	`get radius-user all`

Add Users	add radius-user *`UserName`* username *`UserName`* For example: `add radius-user samantha username samantha`
To set the user's real name:	set radius-user *`UserName`* realname *`RealName`* For example: `set radius-user samantha realname "Elizabeth Montgomery"` (or `set radius-user samantha realname Elizabeth`)
To set user's password:	set radius-user *`UserName`* password *`Password`* For example: `set radius-user samantha password westport`
Enable a user account	set radius-user *`UserName`* disabled 0 For example: `set radius-user samantha disabled 0`
Disable a user account	set radius-user *`UserName`* disabled 1 For example: `set radius-user samantha disabled 1`
Remove a User Account	`remove radius-user` *`UserName`*

Note The user account requires a value for the **disabled** parameter. If a single user is missing a value for **disabled**, the user account table in the Web User Interface will not display any users.

Get All User Accounts

To view all user names:

```
USR5453-AP# get radius-user all name
name
---------
larry
```

To view all user accounts:

```
USR5453-AP# get radius-user all
```

```
name      username  disabled  password  realname
------------------------------------------------------------
larry     larry     0                   David White
```

(At the start, "larry" is the only user configured.)

Add Users

In this example, you will add four new users: (1) samantha, (2) endora, (3) darren, and (4) wally. You will set up user names, real names, and passwords for each.

1. Add **username** "samantha":

   ```
   USR5453-AP# add radius-user samantha username samantha
   ```

2. Provide a **real name** (Elizabeth Montgomery) for this user:

   ```
   USR5453-AP# set radius-user samantha realname "Elizabeth Montgomery"
   ```

3. Set the user **password** for samantha to "westport":

   ```
   USR5453-AP# set radius-user samantha password westport
   ```

4. Enable user "samantha":

   ```
   USR5453-AP# set radius-user samantha disabled 0
   ```

5. Repeat this process to add some other users (endora, darren, and wally):

   ```
   USR5453-AP# add radius-user endora username endora
   USR5453-AP# set radius-user endora realname "Agnes Moorhead"
   USR5453-AP# set radius-user endora password scotch
   USR5453-AP# set radius-user endora disabled 0
   USR5453-AP# add radius-user darren username darren
   USR5453-AP# set radius-user darren realname "Dick York"
   USR5453-AP# set radius-user darren password martini
   USR5453-AP# set radius-user darren disabled 0
   USR5453-AP# add radius-user wally username wally
   USR5453-AP# set radius-user wally realname "Tony Dow"
   USR5453-AP# set radius-user wally password sodapop
   USR5453-AP# set radius-user wally disabled 0
   ```

6. After configuring these new accounts, use the "**get**" command to view all users. (Passwords are always hidden.)

   ```
   USR5453-AP# get radius-user all
   name      username  disabled  password  realname
   ------------------------------------------------------------
   larry     larry     0                   David White
   samantha  samanatha 0                   Elizabeth Montgomery
   endora    endora    0                   Agnes Moorhead
   darren    darren    0                   Dick York
   wally     wally     0                   Tony Dow
   ```

Remove a User Account

To remove a user account, type the following

```
USR5453-AP# remove radius-user wally
```

Use the "**get**" command to view all user names. (You can see "wally" has been removed.)

```
USR5453-AP# get radius-user all name
name
--------
larry
samantha
endora
darren
```

Status

The command tasks and examples in this section show status information on access points. These settings correspond to what is shown on the Status tabs in the Web User Interface. ("Status" on page 77)

This table provides a quick view of all Status commands and links to detailed examples.

Note Make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 190. The interface name you reference in a **get** command determines whether the command output shows a wired or wireless interface or the Internal or Guest network.

This table shows a quick view of Status commands and provides links to detailed examples

Status Command	Example
Understanding Interfaces as Presented in the CLI	Reference of interface names and purposes as described in "Understanding Interfaces as Presented in the CLI" on page 190.
Global command to get all detail on a Basic Service Set (BSS). This is a useful command to use to get a comprehensive understanding of how the access point is currently configured.	`get bss all detail`
Get Common Information on the Internal Interface for the Access Point	`get interface br0`
Get All Wired Settings for the Wired Internal Interface	`get interface br0`

Get Current Settings for the Ethernet (Wired) Guest Interface	`get interface brguest`
	`get interface brguest mac`
	`get interface brguest ssid`

Get the MAC Address for the Wired Internal Interface	`get interface wlan0 mac`

Status Command	Example
Get the Network Name (SSID) for the Wired Internal Interface	`get interface wlan0 ssid`
Get the Current IEEE 802.11 Radio Mode	`get radio wlan0 mode`
Get the Channel the Access Point is Currently Using	`get radio wlan0 channel`

Get Basic Radio Settings for the Internal Interface	`get radio wlan0`
	`get radio wlan0 detail`

Get Status on Events	`get log-entry`
Enable Remote Logging and Specify the Log Relay Host for the Kernel Log	As a prerequisite to remote logging, the Log Relay Host must be configured first as described in Setting Up the Log Relay Host. See complete explanation of CLI commands at Enable Remote Logging and Specify the Log Relay Host for the Kernel Log. Here are a few: `set log relay-enabled 1` enables remote logging `set log relay-enabled 1` disables remote logging `get log` `set log` TAB TAB shows values you can set on the log
Get Transmit / Receive Statistics	`get interface all ip mac ssid tx-packets tx-bytes tx-errors rx-packets rx-bytes rx-errors`
Get Client Associations	`get association`
Get neighbouring Access Points	`get clustered-ap`

Get Common Information on the Internal Interface for the Access Point

The following command obtains all information on the internal interface for an access point:

```
USR5453-AP# get interface br0
Field           Value
--------------------
type            bridge
status          up
hello           10
mac             00:a0:c9:8c:c4:7e
ip              192.168.1.1
mask            255.255.255.0
```

Get Current Settings for the Ethernet (Wired) Internal Interface

The following example shows how to use the CLI to get the Ethernet (Wired) settings for the Internal interface for an access point. You can see by the output results of the command that the MAC address is 00:a0:c9:8c:c4:7e, the IP address is 192.168.1.1, and the subnet mask is 255.255.255.0.

Get All Wired Settings for the Wired Internal Interface

```
USR5453-AP# get interface br0
```

```
Field          Value
--------------------
mac            00:a0:c9:8c:c4:7e
ip             192.168.1.1
mask           255.255.255.0
```

Get the MAC Address for the Wired Internal Interface

```
USR5453-AP# get interface wlan0 mac
02:0C:41:00:02:00
```

Get the Network Name (SSID) for the Wired Internal Interface

```
USR5453-AP# get interface wlan0 ssid
elliot_AP
```

Get Current Settings for the Ethernet (Wired) Guest Interface

The following example shows how to use the CLI to get the Ethernet (Wired) settings for the Guest interface for an access point. You can see by the output results of the command that the MAC address is 00:50:04:6f:6f:90, the IP address is 10.10.56.248, and the subnet mask is 255.255.255.0.

```
USR5453-AP# get interface brguest
Field         Value
--------------------
type          bridge
status        up
mac           00:50:04:6f:6f:90
ip            10.10.56.248
mask          255.255.255.0
```

Note

You can get specifics on the Guest interface by using the same types of commands as for the Internal interface but substituting `brguest` for `wlan0`. For example, to get the MAC address for the guest interface: `get interface wlan0 ssid`

Get Current Wireless (Radio) Settings

The following examples show how to use the CLI to get wireless radio settings on an access point, such as mode, channel, and so on. You can see by the results of the commands that the access point mode is set to IEEE 802.11g, the channel is set to 6, the beacon interval is 100, and so forth.

For information on how to configure Radio settings through the CLI, see “Radio Settings” on page 230.

(Radio settings are fully described in “Configuring Radio Settings” on page 130.)

Get the Current IEEE 802.11 Radio Mode

```
USR5453-AP# get radio wlan0 mode
g
```

Get the Channel the Access Point is Currently Using

```
USR5453-AP# get radio wlan0 channel
2
```

Get Basic Radio Settings for the Internal Interface

```
USR5453-AP# get radio wlan0
Field                    Value
```

```
------------------------------
status                   up
max-bsses                2
channel-policy           best
channel                  6
static-channel           9
mode                     g
fragmentation-threshold  2346
rts-threshold            2347
ap-detection             on
beacon-interval          100
```

Get All Radio Settings on the Internal Interface

```
USR5453-AP# get radio wlan0 detail
Field                                    Value
----------------------------------------------------
status                                   up
description                              IEEE 802.11
mac
max-bss                                  2
channel-policy                           best
mode                                     g
static-channel                           11
channel                                  2
tx-power                                 100
tx-rx-status                             up
beacon-interval                          100
rts-threshold                            2347
fragmentation-threshold                  2346
load-balance-disassociation-utilization  0
load-balance-disassociation-stations     0
load-balance-no-association-utilization  0
ap-detection                             on
station-isolation                        off
frequency                                2417
wme                                      on
```

Get Status on Events

```
USR5453-AP# get log-entry
Number  Time             Priority  Daemon
        Message
------------------------------------------------------
1       Apr 20 21:39:55    debug     udhcpc
        Sending renew...
2       Apr 20 21:39:55    info      udhcpc
        Lease of 10.10.55.216 obtained, lease time 300
3       Apr 20 21:37:25    debug     udhcpc
        Sending renew...
4       Apr 20 21:37:25    info      udhcpc
        Lease of 10.10.55.216 obtained, lease time 300
5       Apr 20 21:34:55    debug     udhcpc
        Sending renew...
6       Apr 20 21:34:55    info      udhcpc
```

```
          Lease of 10.10.55.216 obtained, lease time 300
```

Enable Remote Logging and Specify the Log Relay Host for the Kernel Log

The Kernel Log is a comprehensive list of system even its and kernel messages such as error conditions like dropping frames. To capture Access Point Kernel Log messages you need access to a remote syslog server on the network. The following sections describe how to set up remote logging for the access point.

1. Prerequisites for Remote Logging
2. View Log Settings
3. Enable / Disable Log Relay Host
4. Specify the Relay Host
5. Specify the Relay Port
6. Review Log Settings After Configuring Log Relay Host

Prerequisites for Remote Logging

To capture Kernel Log messages from the access point system, you must first set up a remote server running a syslog process and acting as a syslog "log relay host" on your network. (For information on how to set up the remote server, see “Setting Up the Log Relay Host” on page 80.)

Then, you can use the CLI to configure the Professional Access Point to send its syslog messages to the remote server.

View Log Settings

To view the current log settings:

```
USR5453-AP# get log
Field          Value
--------------------------
depth          15
relay-enabled 0
relay-host
relay-port     514
```

When you start a new access point, the Log Relay Host is disabled. From the above output for the "`get log`" command, you can identify the following about the Log Relay Host (syslog server):

- The syslog server is *disabled* (because "relay-enabled" is set to "0")
- No IP address or Host Name is specified for the syslog server.
- The access point is listening for syslog messages on the default port 514

Enable / Disable Log Relay Host

To enable the Log Relay Host:

```
USR5453-AP# set log relay-enabled 1
```

To disable the Log Relay Host:

```
USR5453-AP# set log relay-enabled 0
```

Specify the Relay Host

To specify the Relay Host, provide either the IP Address or a DNS name for the Log Relay Host as parameters to the "**set log relay-host**" command as shown below.

Note If you are using Instant802 Conductor, the Repository Server should receive the syslog messages from all access points. In this case, use the IP address of the Conductor Repository Server as the Relay Host.

- To specify an IP address for the syslog server:

  ```
  set log relay-host IP_Address_Of_LogRelayHost
  ```

  Where *IP_Address_Of_LogRelayHost* is the IP Address of the Log Relay Host.

  For example:

  ```
  USR5453-AP# set log relay-host 10.10.5.220
  ```
- To specify a Host Name for the syslog server:

  ```
  set log relay-host Host_Name_Of_LogRelayHost
  ```

  Where *Host_Name_Of_LogRelayHost* is the a DNS name for the Log Relay Host.

  For example:

  ```
  USR5453-AP# set log relay-host myserver
  ```

Specify the Relay Port

To specify the Relay Port for the syslog server:

```
set log relay-port Number_Of_LogRelayPort
```

Where *Number_Of_LogRelayPort* is the port number for the Log Relay Host.

For example:

```
USR5453-AP# set log relay-port 514
```

Review Log Settings After Configuring Log Relay Host

To view the current log settings:

```
USR5453-AP# get log
Field          Value
--------------------------
depth          15
relay-enabled  1
relay-host     10.10.5.220
relay-port     514
```

From the above output for the "`get log`" command, you can identify the following about the Log Relay Host (syslog server):

- The syslog server is *enabled* (because "relay-enabled" is set to "1")
- The syslog server is at the IP address `10.10.5.220`
- The access point is listening for syslog messages on the default port 514

Get Transmit / Receive Statistics

```
USR5453-AP# get interface all ip mac ssid tx-packets tx-bytes tx-errors rx-packets
rx-bytes rx-errors
Name        Ip            Mac                Ssid               Tx-packets
            Tx-bytes  Tx-errors  Rx-packets  Rx-bytes  Rx-errors
---------------------------------------------------------------------------
lo          127.0.0.1     00:00:00:00:00:00                     1319
             151772   0          1319        151772   0
eth0                      00:A0:C9:8C:C4:7E                     4699
            3025566   0         11323       1259824   0
eth1        0.0.0.0       00:50:04:6F:6F:90                      152
              49400   0          6632        664298   0
br0         10.10.55.216  00:A0:C9:8C:C4:7E                     4699
            3025566   0         10467        885264   0
brguest     10.10.56.248  00:50:04:6F:6F:90                      152
              48032   0          5909        293550   0
wlan0       0.0.0.0       02:0C:41:00:02:00  AAP1000 (Trusted)  6483
             710681   0             0             0   0
wlan0guest  0.0.0.0       02:0C:41:00:02:01  AAP1000 (Guest)    5963
             471228   0             0             0   0
wlan0wds0
wlan0wds1
wlan0wds2
wlan0wds3
```

Get Client Associations

```
USR5453-AP# get association
Interf Station            Authen Associ Rx-pac Tx-pac Rx-byt Tx-byt Tx-rat
wlan0  00:0c:41:8f:a7:72  Yes    Yes    126    29      9222   3055  540
wlan0  00:09:5b:2f:a5:2f  Yes    Yes    382    97     16620  10065  110
USR5453-AP# get association detail
Inter  Station            Authe Assoc Rx-pa Tx-pa Rx-byt Tx-byt Tx-ra Liste
wlan0  00:0c:41:8f:a7:72  Yes   Yes   126   29     9222   3055  540   1
wlan0  00:09:5b:2f:a5:2f  Yes   Yes   382   97    16620  10065  110   1
```

Get neighbouring Access Points

The Neighboring access point view shows wireless networks within range of the access point. These commands provide a detailed view of neighboring access points including identifying information (SSIDs and MAC addresses) for each, and statistical information such as the channel each access point is broadcasting on, signal strength, and so forth.

To see the kinds of information about access point neighbours you can search on, type **`get detected-ap`** TAB TAB.

```
USR5453-AP# get detected-ap
[Enter]             * Get common fields *
band                Frequency band
beacon-interval     Beacon interval in kus (1.024 ms)
capability          IEEE 802.11 capability value
channel             Channel
detail              * Get all fields *
erp                 ERP
last-beacon         Time of last beacon
mac                 MAC address
num_beacons         Number of beacons received
phy-type            PHY mode detected with
privacy             WEP or WPA enabled
rate                Rate
signal              Signal strength
ssid                Service Set IDentifier (a.k.a., Network Name)
supported-rates     Supported rates list
type                Type (AP, Ad hoc, or Other)
wpa                 WPA security enabled
```

To get the neighbouring access points, type **`get detected-ap`**.

```
USR5453-AP# get detected-ap
Field    Value
-----------------------------------------
mac      00:e0:b8:76:28:e0
type     AP
privacy  On
ssid     Purina
channel  6
signal   2

Field    Value
-----------------------------------------
mac      00:0e:81:01:01:62
type     AP
privacy  Off
ssid     Internal Instant802 Network
channel  6
signal   1

Field    Value
-----------------------------------------
mac      00:e0:b8:76:1a:f6
type     AP
privacy  Off
ssid     domani
channel  6
signal   3

Field    Value
```

```
-----------------------------------------
mac       00:e0:b8:76:28:c0
type      AP
privacy   Off
ssid      domani
channel   6
signal    4
```

Ethernet (Wired) Interface

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 190. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

This table shows a quick view of commands for getting and setting values for the Wired interface and provides links to detailed examples.

Wired Interface Command	Example
Get Summary View of Internal and Guest Interfaces	`get bss`
Get the DNS Name	`get host id`

Set the DNS Name	`set host id` *`HostName`*
	For example:
	`set host id vicky-ap`

Get Current Settings for the Ethernet (Wired) Internal Interface	`get interface br0`
Get Current Settings for the Ethernet (Wired) Guest Interface	`get interface brguest`
Set Up Guest Access	Setting up Guest Access consists of configuring Internal and Guest Wired interfaces on VLANs. For detailed examples, see "Set Up Guest Access" on page 208.
Find out if Guest Access is enabled and configured.	`get interface brguest status` (will be "up" or "down")
Get/Change the Connection Type (DHCP or Static IP)	See detailed example in "Get/Change the Connection Type (DHCP or Static IP)" on page 211.
Re-Configure Static IP Addressing Values	For detailed examples see: "Set the Static IP Address" on page 212 "Set the Static Subnet Mask Address" on page 212 "Set the Static Subnet Mask Address" on page 212

Wired Interface Command	Example
Set DNS Nameservers to Use Static IP Addresses (Dynamic to Manual Mode)	See example below.
Set DNS Nameservers to Use DHCP IP Addressing (Manual to Dynamic Mode)	See example below.

Get Summary View of Internal and Guest Interfaces

```
USR5453-AP# get bss
name              status  radio  beacon-interface  mac
--------------------------------------------------------------------
wlan0bssInternal  up      wlan0  wlan0             00:0C:41:16:DF:A6
wlan0bssGuest     down    wlan0  wlan0guest
```

Get the DNS Name

```
USR5453-AP# get host id
USR5453-AP
```

Set the DNS Name

```
USR5453-AP# set host id vicky-ap
bob# get host id
vicky-ap
```

Get Wired Internal Interface Settings

See "Get Current Settings for the Ethernet (Wired) Internal Interface" on page 200 under Status.

Get Wired Guest Interface Settings

See "Get Current Settings for the Ethernet (Wired) Guest Interface" on page 201 under Status.

Set Up Guest Access

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 190. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

Configuring a Guest interface from the CLI is a complex task. Unless this is your area of expertise, you may find it easier to use the Web User Interface to set up Guest Access. For information on how to set up Guest Access from the Web User Interface, see "Ethernet (Wired) Settings" on page 89 and "Guest Login" on page 121.

Before configuring guest or internal interface settings, make sure you are familiar the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 190.

Note After you configure the Guest Network (as described in the sections below), you can enable a "captive portal" Welcome page for guest clients who are using the Web over your Guest network. You can modify the Welcome page text that is displayed to guests when they log on to the Web. For more information, see “Enable/Configure Guest Login Welcome Page” on page 228.

The following Guest Access configuration examples are provided:

- Enable / Configure Guest Access on VLANs
- Disable Guest Access on VLANs
- Change VLAN IDs (VLANs Must Be Enabled Already)

Enable / Configure Guest Access on VLANs

Caution

- You cannot use an ssh or telnet connection to configure VLANs, because you will lose network connectivity to the access point when you remove the bridge-port. Therefore, you cannot configure VLANs through the CLI.
- Be sure to verify that the switch and DHCP server you are using can support VLANs per the 802.1Q standard. After configuring the VLAN on the Advanced menu’s Ethernet (Wired) Settings page, physically reconnect the Ethernet cable on the switch to the tagged packet (VLAN) port. Then, re-connect via the Web User Interface to the new IP address. (If necessary, check with the infrastructure support administrator regarding the VLAN and DHCP configurations.)

This example assumes you start with Guest Access "disabled" and provides commands to enable it on VLANs.

1. Get the current status of Guest Access (it is "down" or disabled initially):

```
USR5453-AP# get interface brguest status
down
```

2. Enable Guest and remove bridge-port:

```
USR5453-AP# set bss wlan0bssGuest status up
USR5453-AP# set bss wlan1bssGuest status up
USR5453-AP# set interface brguest status up
USR5453-AP# set portal status up
USR5453-AP# remove bridge-port br0 interface eth0
```

3. Enable VLANs:

```
USR5453-AP# add interface vlan1111 type vlan status up vlan-id 1111 vlan-interface
eth0
USR5453-AP# add bridge-port br0 interface vlan1111
USR5453-AP# add interface vlan2222 type vlan status up vlan-id 2222 vlan-interface
eth0
USR5453-AP# add bridge-port brguest interface vlan2222
```

4. Check the current settings:

```
USR5453-AP# get bss
```

```
name              status  radio  beacon-interface  mac
--------------------------------------------------------------------
wlan0bssInternal  up      wlan0  wlan0             00:01:02:03:04:01
wlan0bssGuest     up      wlan0  wlan0guest        00:01:02:03:04:02

USR5453-AP# get interface brguest
Field   Value
-------------------------
type    bridge
status  up
mac     00:01:02:03:04:02
ip      10.10.56.248
mask    255.255.255.0
```

Disable Guest Access on VLANs

This example assumes you start with Guest Access "enabled" on VLANs and provides commands to disable it.

1. Get the current status of Guest Access (it is "up" or enabled initially):

   ```
   USR5453-AP# get interface brguest status
   up
   ```

   The output for the following commands show that VLANs are configured for the Internal and Guest interfaces (because both interfaces are VLANs: "`brguest`" is `vlan2222` and "`br0`" is `vlan1111`):

   ```
   USR5453-AP# get bridge-port brguest
   Name     Interface
   -------------------
   brguest  wlan0
   brguest  vlan2222

   USR5453-AP# get bridge-port br0
   Name  Interface
   ---------------
   br0   wlan0guest
   br0   vlan1111
   ```

2. The following series of commands reconfigures the Internal interface to use an Ethernet port (by setting `br0` to `eth0`), disables Guest Access, and removes the two VLANs.

   ```
   USR5453-AP# add bridge-port br0 interface eth0
   USR5453-AP# set bss wlan0bssGuest status down
   USR5453-AP# set bss wlan1bssGuest status down
   USR5453-AP# remove bridge-port br0 interface vlan1111
   USR5453-AP# remove interface vlan1111
   USR5453-AP# remove bridge-port brguest interface vlan2222
   USR5453-AP# remove interface vlan2222
   USR5453-AP# set interface brguest status down
   USR5453-AP# set portal status down
   ```

Change VLAN IDs (VLANs Must Be Enabled Already)

1. Check the current configuration of Wired interfaces.

   The output of the following command shows that the Guest interface is already configured on VLANs:

```
USR5453-AP# get bridge-port br0
Name  Interface
---------------
br0   wlan0guest
br0   vlan1111
```

2. Set up a new VLAN and remove the old one:

```
USR5453-AP# set interface vlan1111 vlan-id 1112
Error: vlan-id cannot be changed after insert.
USR5453-AP# remove bridge-port br0 interface vlan1111
USR5453-AP# remove interface vlan1111
USR5453-AP# add interface vlan1113 type vlan status up vlan-id 1113 vlan-interface
eth0
```

Get/Change the Connection Type (DHCP or Static IP)

Note For more information on DHCP and Static IP connection types, see the topic "“Understanding Dynamic and Static IP Addressing on the Professional Access Point” on page 20.

To get the connection type:

```
USR5453-AP# get dhcp-client status
up
```

You cannot use the CLI to reset the connection type from DHCP to Static IP because you will lose connectivity during the process of assigning a new static IP address. To make such a change, use the Web User Interface on a computer connected to the access point with an Ethernet cable.

To reset the connection type from Static IP to DHCP:

```
USR5453-AP# set dhcp-client status up
```

To view the new settings:

```
USR5453-AP# get interface br0 detail
Field                Value
-----------------------------------
type                 bridge
status               up
description          Bridge - Internal
mac                  00:E0:B8:76:23:B4
ip                   10.10.12.221
mask                 255.255.255.0
static-ip            10.10.12.221
static-mask          255.255.255.0
nat
```

Re-Configure Static IP Addressing Values

Note This section assumes you have already set the access point to use Static IP Addressing and set some initial values as described in “Get/Change the Connection Type (DHCP or Static IP)” on page 211.

If you are using static IP addressing on the access point (instead of DHCP), you may want to reconfigure the static IP address, subnet mask, default gateway, or DNS name servers.

The following examples show how to change these values from the CLI. With the exception of DNS name servers, these values can only be reconfigured if you are using Static IP Addressing mode.

You do have the option of manually configuring DNS name servers for either a DHCP or Static IP connection type, so that task is covered in a separate section following this one.

Set the Static IP Address

1. Check to see what the current static IP address is. (In this example, the current static IP address is the factory default.)

```
USR5453-AP# get interface br0 static-ip
10.10.12.221
```

2. Re-set to a new static IP address:

```
USR5453-AP# set interface br0 static-ip 10.10.12.81
```

Set the Static Subnet Mask Address

1. Check to see the current Subnet Mask. (In this example, the current subnet mask is the factory default.)

```
USR5453-AP# get interface br0 static-mask
255.255.255.0
```

2. Re-set to a new static Subnet Mask:

```
USR5453-AP# set interface br0 static-mask 255.255.255.128
```

Set the IP Address for the Default Gateway

This example sets the Default Gateway to 10.10.12.126:

```
USR5453-AP# set ip-route with gateway 10.10.12.126 in-use yes
```

Set DNS Nameservers to Use Static IP Addresses (Dynamic to Manual Mode)

This example shows how to reconfigure DNS Nameservers from *Dynamic* mode (where name server IP addresses are assigned through DHCP) to *Manual* mode, and specify static IP addresses for them.

1. Check to see which mode the DNS Name Service is running in. (In this example, DNS naming is running in DHCP mode initially because the following command returns `up` for the mode.)

```
USR5453-AP# get host dns-via-dhcp
up
```

2. Turn off Dynamic DNS Nameservers and re-check the settings:

```
USR5453-AP# set host dns-via-dhcp down
USR5453-AP# get host dns-via-dhcp
down
```

3. Get the current IP addresses for the DNS Nameservers:

```
USR5453-AP# get host static-dns-1
10.10.3.9

USR5453-AP# get host static-dns-2
10.10.3.11
```

4. Re-set the IP addresses for the DNS Nameservers as desired:

```
USR5453-AP# set host static-dns-1 10.10.3.10
USR5453-AP# get host static-dns-1
10.10.3.10

USR5453-AP# set host static-dns-2 10.10.3.12
USR5453-AP# get host static-dns-2
10.10.3.12
```

Set DNS Nameservers to Use DHCP IP Addressing (Manual to Dynamic Mode)

To switch DNS Nameservers from Manual (static IP addresses) to Dynamic mode (nameserver addresses assigned by DHCP), use the reverse command and check to see the new configuration:

```
USR5453-AP# set host dns-via-dhcp up
USR5453-AP# get host dns-via-dhcp
up
```

Wireless Interface

To set up a wireless (radio) interface, configure the following on each interface (Internal or Guest) as described in other sections of this CLI document.

- Configure the Radio Mode and Radio Channel as described in “Configure Radio Settings” on page 232.
- Configure the Network Name as described in “Set the Wireless Network Name (SSID)” on page 195.

Security

Note

Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 190. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

The following sections show examples of how to use the CLI to view and configure security settings on the access point. These settings correspond to those available in the Web User Interface on the Advanced menu's Security tab. For a detailed discussion of concepts and configuration options, see"Security" on page 101.

This section focuses on configuring security on the *Internal* network. (Security on the *Guest* network defaults to **None**. See "When to Use No Security" on page 102.)

This table shows a quick view of Security commands and links to detailed examples.

Security Command	Example
Get the Current Security Mode	`get interface wlan0 security`

Get Detailed Description of Current Security Settings	`get bss wlan0bssInternal detail`
	`get interface wlan0 detail`

Set the Broadcast SSID (Allow or Prohibit)	`set bss wlan0bssInternal ignore-broadcast-ssid on`
	`set bss wlan0bssInternal ignore-broadcast-ssid off`

Enable / Disable Station Isolation	
Set Security to None	`set interface wlan0 security plain-text`
Set Security to Static WEP	See detailed example in "Set Security to Static WEP" on page 216.
Set Security to IEEE 802.1x	See detailed example in"Set Security to IEEE 802.1x" on page 219.
Set Security to WPA/WPA2 Personal (PSK)	See detailed example in "Set Security to WPA/WPA2 Personal (PSK)" on page 221.
Set Security to WPA/WPA2 Enterprise (RADIUS)	See detailed example in "Set Security to WPA/WPA2 Enterprise (RADIUS)" on page 223.

Get the Current Security Mode

```
USR5453-AP# get interface wlan0 security
none
```

Get Detailed Description of Current Security Settings

```
USR5453-AP# get bss wlan0bssInternal detail
Field                         Value
---------------------------------------------
status                        up
description                   Internal
radio                         wlan0
beacon-interface              wlan0
mac                           00:0C:41:16:DF:A6
dtim-period
max-stations
ignore-broadcast-ssid         off
mac-acl-mode                  deny-list
mac-acl-name                  wlan0bssInternal
radius-accounting
```

```
   radius-ip                   127.0.0.1
   radius-key                  secret
   open-system-authentication
   shared-key-authentication
   wpa-cipher-tkip
   wpa-cipher-ccmp
   wpa-allowed                 off
   wpa2-allowed                off
   rsn-preauthentication
```

Set the Broadcast SSID (Allow or Prohibit)

To set the Broadcast SSID to on (allow):

```
   USR5453-AP# set bss wlan0bssInternal ignore-broadcast-ssid on
```

To set the Broadcast SSID to off (prohibit):

```
   USR5453-AP# set bss wlan0bssInternal ignore-broadcast-ssid off
```

Enable / Disable Station Isolation

```
   USR5453-AP# get radio wlan0 station-isolation
   off
   USR5453-AP# set radio wlan0 station-isolation off
   USR5453-AP# get radio wlan0 detail
   Field                                    Value
   ---------------------------------------------------------------
   status                                   up
   description                              Radio 1 - IEEE 802.11g
   mac
   max-bss                                  4
   channel-policy                           static
   mode                                     g
   static-channel                           6
   channel                                  6
   tx-power                                 100
   tx-rx-status                             up
   beacon-interval                          100
   rts-threshold                            2347
   fragmentation-threshold                  2346
   load-balance-disassociation-utilization  0
   load-balance-disassociation-stations     0
   load-balance-no-association-utilization  0
   ap-detection                             off
   station-isolation                        off
   frequency                                2437
   wme                                      on
```

Set Security to None

```
    USR5453-AP# set interface wlan0 security none
```

Set Security to Static WEP

1. Set the Security Mode

```
    USR5453-AP# set interface wlan0 security static-wep
```

2. Set the Transfer Key Index

The following commands set the Transfer Key Index to 4.

```
    USR5453-AP# set interface wlan0 wep-default-key 1
    USR5453-AP# set interface wlan0 wep-default-key 2
    USR5453-AP# set interface wlan0 wep-default-key 3
    USR5453-AP# set interface wlan0 wep-default-key 4
```

3. Set the Key Length

For the CLI, valid values for Key Length are 40 bits or 104 bits.

Note The Key Length values used by the CLI do not include the initialisation vector in the length. On the Web User Interface, longer Key Length values may be shown which include the 24-bit initialisation vector. A Key Length of 40 bits (not including initialisation vector) is equivalent to a Key Length of 64 bits (with initialisation vector). A Key Length of 104 bits (not including initialisation vector) is equivalent to a Key Length of 128 bits (which includes the initialisation vector).

To set the WEP Key Length, type one of the following commands:

To set the WEP Key Length to 40 bits:	`set interface wlan0 wep-key-length 40`
To set the WEP Key Length to 104 bits:	`set interface wlan0 wep-key-length 104`

In this example, you will set the WEP Key Length to 40.

```
    USR5453-AP# set interface wlan0 wep-key-length 40
```

4. Set the Key Type

Valid values for Key Type are ASCII or Hex. The following commands set the Key Type.

To set the Key Type to ASCII:	`set interface wlan0 wep-key-ascii yes`
To set the Key Type to Hex:	`set interface wlan0 wep-key-ascii no`

In this example, you will set the Key Type to ASCII:

```
USR5453-AP# set interface wlan0 wep-key-ascii yes
```

5. Set the WEP Keys

Note The number of characters required for each WEP key depends on how you set Key Length and Key Type:

- If Key Length is 40 bits and the Key Type is "ASCII", then each WEP key be 5 characters long.
- If Key Length is 40 bits and Key Type is "Hex", then each WEP key must be 10 characters long.
- If Key Length is 104 bits and Key Type is "ASCII", then each WEP Key must be 13 characters long.
- If Key Length is 104 bits and Key Type is "Hex", then each WEP Key must be 26 characters long.

Although the CLI will allow you to enter WEP keys of any number of characters, you must use the correct number of characters for each key to ensure a valid security configuration.

```
USR5453-AP# set interface wlan0 wep-key-1 abcde
USR5453-AP# set interface wlan0 wep-key-2 fghi
USR5453-AP# set interface wlan0 wep-key-3 klmno
USR5453-AP# set interface wlan0 wep-key-4
```

6. Set the Authentication Algorithm

The options for the authentication algorithm are Open System, Shared Key or Both:

To set Authentication Algorithm to **Open System**:	`set bss wlan0bssInternal open-system-authentication on`
	`set bss wlan0bssInternal shared-key-authentication off`

To set Authentication Algorithm to **Shared Key**:	`set bss wlan0bssInternal open-system-authentication off`
	`set bss wlan0bssInternal shared-key-authentication on`

To set Authentication Algorithm to **Both**:	`set bss wlan0bssInternal open-system-authentication on`
	`set bss wlan0bssInternal shared-key-authentication on`

In this example, you will set the authentication algorithm to Shared Key:

```
USR5453-AP# set bss wlan0bssInternal shared-key-authentication on
USR5453-AP# set bss wlan0bssInternal open-system-authentication off
```

7. Get Current Security Settings After Re-Configuring to Static WEP Security Mode

Now you can use the "get" command again to view the updated security configuration and see the results of your new settings.

The following command gets the security mode in use on the Internal network:

```
USR5453-AP# get interface wlan0 security
static-wep
```

The following command gets details on how the internal network is configured, including details on

Security.

```
USR5453-AP# get bss wlan0bssInternal detail
Field                       Value
---------------------------------------------
status                      up
description                 Internal
radio                       wlan0
beacon-interface            wlan0
mac                         00:0C:41:16:DF:A6
dtim-period                 2
max-stations                2007
ignore-broadcast-ssid       off
mac-acl-mode                deny-list
mac-acl-name                wlan0bssInternal
radius-accounting           off
radius-ip                   127.0.0.1
radius-key                  secret
open-system-authentication  off
shared-key-authentication   on
wpa-cipher-tkip             off
wpa-cipher-ccmp             off
wpa-allowed                 off
wpa2-allowed                off
rsn-preauthentication       off
```

The following command gets details on the interface and shows the WEP Key settings, specifically.

```
USR5453-AP# get interface wlan0 detail
Field             Value
-------------------------------------------
type              service-set
status            up
description       Wireless - Internal
mac               00:0C:41:16:DF:A6
ip                0.0.0.0
static-ip         0.0.0.0
static-mask
nat
rx-bytes          0
rx-packets        0
rx-errors         0
rx-drop           0
rx-fifo           0
rx-frame          0
rx-compressed     0
rx-multicast      0
tx-bytes          259662
tx-packets        722
tx-errors         0
tx-drop           0
tx-fifo           0
tx-colls          0
tx-carrier        0
```

```
tx-compressed      0
ssid               Vicky's AP
bss                wlan0bssInternal
security           static-wep
wpa-personal-key
wep-key-ascii      yes
wep-key-length     104
wep-default-key    4
wep-key-1          abcde
wep-key-2          fghij
wep-key-3          klmno
wep-key-4
vlan-interface
vlan-id
radio
remote-mac
wep-key
```

Set Security to IEEE 802.1x

1. Set the Security Mode

```
USR5453-AP# set interface wlan0 security dot1x
```

2. Set the Authentication Server

You can use the built-in authentication server on the access point or an external RADIUS server.

Note To use the built-in authentication server, set the RADIUS IP address to that used by the built-in server (`127.0.0.1`) and turn RADIUS accounting off (because it is not supported by the built-in server)

RADIUS Option	Example
To set the AP to use the **Built-in** Authentication Server:	`set bss wlan0bssInternal radius-ip 127.0.0.1`
To set the AP to use an **External** RADIUS Server:	`set bss wlan0bssInternal radius-ip` *`RADIUS_IP_Address`* where *`RADIUS_IP_Address`* is the IP address of an external RADIUS server.

In this example, you will set it to use the built-in server:

```
USR5453-AP# set bss wlan0bssInternal radius-ip 127.0.0.1
```

3. Set the RADIUS Key (For External RADIUS Server Only)

If you use an external RADIUS server, you must provide the RADIUS key. (If you use the built-in authentication server the RADIUS key is automatically provided.)

This command sets the RADIUS key to `secret` for an external RADIUS server.

```
USR5453-AP# set bss wlan0bssInternal radius-key secret
```

4. Enable RADIUS Accounting (External RADIUS Server Only)

You can enable RADIUS Accounting if you want to track and measure the resources a particular user has consumed such system time, amount of data transmitted and received, and so on.

Note

RADIUS accounting is not supported by the built-in server, so if you are using the built-in server make sure that RADIUS accounting is off.

To enable RADIUS accounting:	`set bss wlan0bssInternal radius-accounting on`
To disable RADIUS accounting:	`set bss wlan0bssInternal radius-accounting off`

In this example, you will disable RADIUS accounting since you are using the built-in server:

```
USR5453-AP# set bss wlan0bssInternal radius-accounting off
```

5. Get Current Security Settings After Re-Configuring to IEEE 802.1x Security Mode

Now you can use the "get" command again to view the updated security configuration and see the results of your new settings.

The following command gets the security mode in use on the Internal network:

```
USR5453-AP# get interface wlan0 security
dot1x
```

The following command gets details on how the internal BSS is configured, including details on Security.

```
USR5453-AP# get bss wlan0bssInternal detail
Field                        Value
---------------------------------------------
status                       up
description                  Internal
radio                        wlan0
beacon-interface             wlan0
mac                          00:0C:41:16:DF:A6
dtim-period                  2
max-stations                 2007
ignore-broadcast-ssid        off
mac-acl-mode                 deny-list
mac-acl-name                 wlan0bssInternal
radius-accounting            off
radius-ip                    127.0.0.1
radius-key                   secret
open-system-authentication   off
shared-key-authentication    on
```

```
    wpa-cipher-tkip             off
    wpa-cipher-ccmp             off
    wpa-allowed                 off
    wpa2-allowed                off
    rsn-preauthentication       off
```

Set Security to WPA/WPA2 Personal (PSK)

1. Set the Security Mode

```
    USR5453-AP# set interface wlan0 security wpa-personal
```

2. Set the WPA Versions

Select the WPA version based on what types of client stations you want to support.

WPA Option	Example

WPA: If all client stations on the network support the original WPA but none support the newer WPA2, then use WPA.
To support WPA clients:
	`set bss wlan0bssInternal wpa-allowed on`
	`set bss wlan0bssInternal wpa2-allowed off`

WPA2: If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.
To support WPA2 clients:
	`set bss wlan0bssInternal wpa-allowed off`
	`set bss wlan0bssInternal wpa2-allowed on`

Both: If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select "Both". This lets both WPA and WPA2 client stations assoicate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
To support both WPA and WPA2 clients:
	`set bss wlan0bssInternal wpa-allowed on`
	`set bss wlan0bssInternal wpa2-allowed on`

In this example, you will set the access point to support **Both** WPA and WPA2 client stations:

```
USR5453-AP# set bss wlan0bssInternal wpa-allowed on
USR5453-AP# set bss wlan0bssInternal wpa2-allowed on
```

3. Set the Cipher Suites

Set the cipher suite you want to use. The options are:

Cipher Suite Option	Example

TKIP: Temporal Key Integrity Protocol (TKIP), which is the default.
To set the cipher suite to **TKIP only**:
	`set bss wlan0bssInternal wpa-cipher-tkip on`
	`set bss wlan0bssInternal wpa-cipher-ccmp off`

CCMP (AES) - Counter mode/ CBC-MAC Protocol (CCMP) is an encryption method for IEEE 802.11i that uses the Advanced Encryption Algorithm (AES).
To set the cipher suite to **CCMP (AES) only**:
	`set bss wlan0bssInternal wpa-cipher-tkip off`
	`set bss wlan0bssInternal wpa-cipher-ccmp on`

Both - When the authentication algorithm is set to "**Both**", both TKIP and AES clients can associate with the access point. WPA clients must have either a valid TKIP key or a valid CCMP (AES) key to be able to associate with the AP.
To set the cipher suite to **Both**:
	`set bss wlan0bssInternal wpa-cipher-tkip on`
	`set bss wlan0bssInternal wpa-cipher-ccmp on`

In this example, you will set the cipher suite to **Both**:

```
USR5453-AP# set bss wlan0bssInternal wpa-cipher-tkip on
USR5453-AP# set bss wlan0bssInternal wpa-cipher-ccmp on
```

4. Set the Pre-shared Key

The *Pre-shared Key* is the shared secret key for WPA-PSK. Enter a string of at least 8 characters to a maximum of 63 characters. Following are two examples; the first sets the key to "`SeCret !`", the second sets the key to "`KeepSecret`".

```
Ex 1. USR5453-AP# set interface wlan0 wpa-personal-key "SeCret !"
```

or

```
Ex 2. USR5453-AP# set interface wlan0 wpa-personal-key KeepSecret
```

Note Shared secret keys can include spaces and special characters if the key is placed inside quotation marks as in the first example above. If the key is a string of characters with no spaces or special characters in it, the quotation marks are not necessary as in the second example above..

5. Get Current Security Settings After Re-Configuring to WPA/WPA2 Personal (PSK)

Now you can use the "get" command again to view the updated security configuration and see the results of your new settings.

The following command gets the security mode in use on the Internal network:

```
USR5453-AP# get interface wlan0 security
wpa-personal
```

The following command gets details on how the internal network is configured, including details on Security.

```
USR5453-AP# get bss wlan0bssInternal detail
Field                        Value
---------------------------------------------
status                       up
description                  Internal
radio                        wlan0
beacon-interface             wlan0
mac                          00:0C:41:16:DF:A6
dtim-period
max-stations
ignore-broadcast-ssid        off
mac-acl-mode                 deny-list
mac-acl-name                 wlan0bssInternal
radius-accounting
radius-ip                    127.0.0.1
radius-key                   secret
open-system-authentication
shared-key-authentication
wpa-cipher-tkip              on
wpa-cipher-ccmp              on
wpa-allowed                  on
wpa2-allowed                 on
rsn-preauthentication
```

Set Security to WPA/WPA2 Enterprise (RADIUS)

1. Set the Security Mode
2. Set the WPA Versions
3. Enable Pre-Authentication
4. Set the Cipher Suites
5. Set the Authentication Server
6. Set the RADIUS Key (For External RADIUS Server Only)
7. Enable RADIUS Accounting (External RADIUS Server Only))
8. Get Current Security Settings After Re-Configuring to WPA/WPA2 Enterprise (RADIUS)

8. Get Current Security Settings After Re-Configuring to WPA/WPA2 Enterprise (RADIUS)

1. Set the Security Mode

```
USR5453-AP# set interface wlan0 security wpa-enterprise
```

2. Set the WPA Versions

Select the WPA version based on what types of client stations you want to support.

WPA Option	Example

WPA: If all client stations on the network support the original WPA but none support the newer WPA2, then use WPA.
To support WPA clients:
	`set bss wlan0bssInternal wpa-allowed on`
	`set bss wlan0bssInternal wpa2-allowed off`

WPA2: If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.
To support WPA2 clients:
	`set bss wlan0bssInternal wpa-allowed off`
	`set bss wlan0bssInternal wpa2-allowed on`

Both: If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select "Both". This lets both WPA and WPA2 client stations assoicate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
To support both WPA and WPA2 clients:
	`set bss wlan0bssInternal wpa-allowed on`
	`set bss wlan0bssInternal wpa2-allowed on`

In this example, you will set the access point to support WPA client stations only:

```
USR5453-AP# set bss wlan0bssInternal wpa-allowed on
USR5453-AP# set bss wlan0bssInternal wpa2-allowed off
```

3. Enable Pre-Authentication

If you set WPA versions to "WPA2" or "Both", you can enable *pre-authentication* for WPA2 clients.

Enable pre-authentication if you want WPA2 wireless clients to send pre-authentication packet. The pre-authentication information will be relayed from the access point the client is currently using to the target access point. Enabling this feature can help speed up authentication for roaming clients who connect to multiple access points. To enable pre-authentication for WPA2 clients:	`set bss wlan0bssInternal rsn-preauthentication on`
To disable pre-authentication for WPA2 clients:	set bss wlan0bssInternal rsn-preauthentication on

This option does not apply if you set the WPA Version to support "WPA" clients only because the original WPA does not support this pre-authentication

In this example, you will disable pre-authentication.

```
    USR5453-AP# set bss wlan0bssInternal rsn-preauthentication off
```

4. Set the Cipher Suites

Set the cipher suite you want to use. The options are:

Cipher Suite Option	Example

TKIP: Temporal Key Integrity Protocol (TKIP), which is the default.
To set the cipher suite to **TKIP only**:
	`set bss wlan0bssInternal wpa-cipher-tkip on`
	`set bss wlan0bssInternal wpa-cipher-ccmp off`

CCMP (AES) - Counter mode/ CBC-MAC Protocol (CCMP) is an encryption method for IEEE 802.11i that uses the Advanced Encryption Algorithm (AES).
To set the cipher suite to **CCMP (AES) only**:
	`set bss wlan0bssInternal wpa-cipher-tkip off`
	`set bss wlan0bssInternal wpa-cipher-ccmp on`

Cipher Suite Option	Example

Both - When the authentication algorithm is set to "**Both**", both TKIP and AES clients can associate with the access point. WPA clients must have either a valid TKIP key or a valid CCMP (AES) key to be able to associate with the AP.
To set the cipher suite to **Both**:
	`set bss wlan0bssInternal wpa-cipher-tkip on`
	`set bss wlan0bssInternal wpa-cipher-ccmp on`

In this example, you will set the cipher suite to **TKIP Only**:

```
USR5453-AP# set bss wlan0bssInternal wpa-cipher-tkip on
USR5453-AP# set bss wlan0bssInternal wpa-cipher-ccmp off
```

5. Set the Authentication Server

You can use the built-in authentication server on the access point or an external RADIUS server.

Note To use the built-in authentication server, set the RADIUS IP address to that used by the built-in server (`127.0.0.1`) and turn RADIUS accounting off (because it is not supported by the built-in server)

RADIUS Option	Example
To set the AP to use the **Built-in** Authentication Server:	`set bss wlan0bssInternal radius-ip 127.0.0.1`
To set the AP to use an **External** RADIUS Server:	`set bss wlan0bssInternal radius-ip` *`RADIUS_IP_Address`* where *`RADIUS_IP_Address`* is the IP address of an external RADIUS server.

In this example, you will use an external RADIUS server with an IP address of 142.77.1.1:

```
USR5453-AP# set bss wlan0bssInternal radius-ip 142.77.1.1
```

6. Set the RADIUS Key (For External RADIUS Server Only)

If you use an external RADIUS server, you must provide the RADIUS key. (If you use the built-in authentication server the RADIUS key is automatically provided.)

This command sets the RADIUS key to `KeepSecret` for an external RADIUS server.

```
USR5453-AP# set bss wlan0bssInternal radius-key KeepSecret
```

7. Enable RADIUS Accounting (External RADIUS Server Only)

You can enable RADIUS Accounting if you want to track and measure the resources a particular user has consumed such system time, amount of data transmitted and received, and so on.

Note RADIUS accounting is not supported by the built-in server, so if you are using the built-in server make sure that RADIUS accounting is off.

To enable RADIUS accounting:	`set bss wlan0bssInternal radius-accounting on`
To disable RADIUS accounting:	`set bss wlan0bssInternal radius-accounting off`

For this example, you will enable RADIUS accounting for your external RADIUS server:

```
USR5453-AP# set bss wlan0bssInternal radius-accounting on
```

8. Get Current Security Settings After Re-Configuring to WPA/WPA2 Enterprise (RADIUS)

Now you can use the "get" command again to view the updated security configuration and see the results of your new settings.

The following command gets the security mode in use on the Internal network:

```
USR5453-AP# get interface wlan0 security
wpa-enterprise
```

The following command gets details on how the internal network is configured, including details on Security.

```
USR5453-AP# get bss wlan0bssInternal detail
Field                           Value
---------------------------------------------
status                          up
description                     Internal
radio                           wlan0
beacon-interface                wlan0
mac                             00:0C:41:16:DF:A6
dtim-period                     2
max-stations                    2007
ignore-broadcast-ssid           off
mac-acl-mode                    deny-list
mac-acl-name                    wlan0bssInternal
radius-accounting               on
radius-ip                       142.77.1.1
radius-key                      KeepSecret
open-system-authentication      on
shared-key-authentication       off
wpa-cipher-tkip                 on
wpa-cipher-ccmp                 off
wpa-allowed                     on
wpa2-allowed                    off
rsn-preauthentication           off
```

Enable/Configure Guest Login Welcome Page

Guest Welcome Option	Example
View Guest Login Settings:	`get portal`
Enable/Disable the Guest Welcome Page	`set portal status`
Set Guest Welcome Page Textl:	`set portal welcome-screen-text "`*`Welcome Screen Text`*`"` Where "*Welcome Screen Text*" is the content of the Welcome message you want displayed on the Guest Welcome Web Page. The Welcome message must be in quotes if it contains spaces, punctuation, and special characters."

Note Guest Login settings are only relevant if you have first configured a Guest Network. For information about configuring a Guest Network, see “Set Up Guest Access” on page 208.

You can set up a "captive portal" that Guest clients will see when they log on to the Guest network. or modify the Welcome screen guest clients see when they open a Web browser or try to browse the Web.

View Guest Login Settings

To view the current settings for Guest Login:

```
USR5453-AP# get portal
Field                  Value
---------------------------------------------------------------------------
status                 down
welcome-screen         on
welcome-screen-text    Thank you for using wireless Guest Access as provided
by this U.S. Robotics Corporation wireless AP. Upon clicking "Accept", you
will gain access to our wireless guest network. This network allows complete
access to the Internet but is external to the corporate network. Please note
that this network is not configured to provide any level of wireless
security.
```

Enable/Disable the Guest Welcome Page

To enable the Guest welcome page:

```
USR5453-AP# set portal status up
```

To disable the Guest welcome page:

```
USR5453-AP# set portal status down
```

Set Guest Welcome Page Text

To specify the text for the Guest welcome page:

```
USR5453-AP# set portal welcome-screen-text "Welcome to the Stephens Network"
```

Review Guest Login Settings

The following example shows the results of the "set portal" command after specifying some new settings:

```
USR5453-AP# get portal
Field                  Value
------------------------------------------------------
status                 up
welcome-screen         on
welcome-screen-text    Welcome to the Stephens Network
```

Configuring Multiple BSSIDs on Virtual Wireless Networks

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 190. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network,.

Configuring Virtual Wireless Network "One" on Radio One

1. Configure these settings from the Web User Interface first:

    - On Advanced menu’s Ethernet (Wired) Settings tab on the Web User Interface, enable Virtual Wireless Networks as described in “Enabling and Disabling Virtual Wireless Networks on the Access Point” on page 92.

    - On Advanced menu’s Virtual Wireless Networks tab on the Web User Interface, provide a VLAN ID as described in “Configuring VLANs” on page 126.

2. Use the CLI to configure Security on the interface.

    The following example shows commands for configuring WPA/WPA2 Enterprise (RADIUS) security mode, allowing "Both" WPA and WPA2 clients to authenticate and using a TKIP cipher suite:

```
USR5453-AP# set bss wlan0bssvwn1 open-system-authentication on
USR5453-AP# set bss wlan0bssvwn1 shared-key-authentication on
USR5453-AP# set bss wlan0bssvwn1 wpa-allowed on
USR5453-AP# set bss wlan0bssvwn1 wpa2-allowed on
USR5453-AP# set bss wlan0bssvwn1 wpa-cipher-tkip on
USR5453-AP# set bss wlan0bssvwn1 wpa-cipher-ccmp off
USR5453-AP# set bss wlan0bssvwn1 radius-ip 127.0.0.1
USR5453-AP# set bss wlan0bssvwn1 radius-key secret
USR5453-AP# set bss wlan0bssvwn1 status up
USR5453-AP# set interface wlan0vwn1 security wpa-enterprise
```

3. Use the CLI to set the Network Name (SSID) for the new Virtual Wireless Network:

```
USR5453-AP# set interface wlan0vwn1 ssid my-vwn-one
```

Creating VWN 'Two' on Radio One with WPA security

To configure the second Virtual Wireless Network, repeat steps 1-3 as described above (in Configuring Virtual Wireless Network "One" on Radio One) with the following differences:

- Create a second VLAN ID from the Web User Interface with a new SSID
- In the CLI commands, replace `wlan0bssvwn1` with `wlan0bssvwn2`.

Radio Settings

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 190. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

This table shows a quick view of Radio Settings commands and provides links to detailed examples.

Radio Setting Command	Example

Get Radio Settings	`get radio`
	`get radio wlan0`
	`get radio wlan0 detail`

Get IEEE 802.11 Radio Mode	`get radio wlan0 mode`
Get Radio Channel	`get radio wlan0 channel`
Get Basic Radio Settings	`get radio wlan0`
Get All Radio Settings	`get radio wlan0 detail`
Get Supported Rate Set	`get supported-rate`
Get Basic Rate Set	`get basic-rate`
Configure Radio Settings	See detailed examples in: "1. Turn the Radio On or Off" on page 233 "2. Set the Radio Mode" on page 233 "3. Enable or Disable Super G" on page 233 "4. Set the Beacon Interval" on page 233 "5. Set the DTIM Period" on page 233 "6. Set the Fragmentation Threshold" on page 233 "7. Set the RTS Threshold" on page 234 "8. Configure Basic and Supported Rate Sets" on page 234

Get IEEE 802.11 Radio Mode

To get the current setting for radio Mode:

```
USR5453-AP# get radio wlan0 mode
g
```

(The radio in this example is using IEEE 802.11g mode.)

Get Radio Channel

To get the current setting for radio Channel:

```
USR5453-AP# get radio wlan0 channel
6
```

(The radio in this example is on Channel 6.)

Get Basic Radio Settings

To get basic current Radio settings:

```
USR5453-AP# get radio wlan0
Field           Value
----------------------
status          up
mac
channel-policy  static
mode            g
static-channel  6
channel         6
tx-rx-status    up
```

Get All Radio Settings

To get all current Radio settings: get radio wlan0 detail

```
USR5453-AP# get radio wlan0 detail
Field                                      Value
-----------------------------------------------------
status                                     up
description                                IEEE 802.11
mac
max-bss                                    2
channel-policy                             static
mode                                       g
static-channel                             6
channel                                    6
tx-power                                   100
tx-rx-status                               up
beacon-interval                            100
rts-threshold                              2347
fragmentation-threshold                    2346
load-balance-disassociation-utilization    0
load-balance-disassociation-stations       0
load-balance-no-association-utilization    0
ap-detection                               off
station-isolation                          off
frequency                                  2437
```

```
wme                                         on
```

Get Supported Rate Set

The *Supported Rate Set* is what the access point supports. The access point will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the access point.

```
USR5453-AP# get supported-rate
name   rate
-----------
wlan0  54
wlan0  48
wlan0  36
wlan0  24
wlan0  18
wlan0  12
wlan0  11
wlan0  9
wlan0  6
wlan0  5.5
wlan0  2
wlan0  1
```

Get Basic Rate Set

The *Basic Rate Set* is what the access point will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an access point broadcast a subset of its supported rate sets.

```
USR5453-AP# get basic-rate
name   rate
-----------
wlan0  11
wlan0  5.5
wlan0  2
wlan0  1
```

Configure Radio Settings

Note To get a list of all fields you can set on the access point radio, type the following at the CLI prompt: set radio wlan0 [SpaceKey] [TAB] [TAB]

1. Turn the Radio On or Off
2. Set the Radio Mode
3. Enable or Disable Super G
4. Set the Beacon Interval
5. Set the DTIM Period
6. Set the Fragmentation Threshold
7. Set the RTS Threshold
8. Configure Basic and Supported Rate Sets

1. Turn the Radio On or Off

To turn the radio on:	`set radio wlan0 status up`
To turn the radio off:	`set radio wlan0 status down`

2. Set the Radio Mode

Valid values depend on the capabilities of the radio. Possible values and how you would use the CLI to set each one are shown below.

IEEE 802.11b	set radio wlan0 mode **b**
IEEE 802.11g	set radio wlan0 mode **g**

The following command sets the Wireless Mode to IEEE 802.11g:

```
USR5453-AP# set radio wlan0 mode g
```

3. Enable or Disable Super G

You cannot enable/disable Super G from the CLI. You must set this from the Web User Interface. For information on how to set this option, please see the field description for this option in “Configuring Radio Settings” on page 130.

4. Set the Beacon Interval

The following command sets the beacon interval to 80.

```
USR5453-AP# set radio wlan0 beacon-interval 80
```

5. Set the DTIM Period

The Delivery Traffic Information Map (DTIM) period indicates how often wireless clients should check to see if they have buffered data on the access point awaiting pickup. The measurement is in beacons. Specify a DTIM period within a range of 1 - 255 beacons. For example, if you set this to "1" clients will check for buffered data on the access point at every beacon. If you set this to "2", clients will check on every other beacon.

The following command sets the DTIM interval to 3.

```
USR5453-AP# set bss wlan0bssInternal dtim-period 3
```

To get the updated value for DTIM interval after you have changed it:

```
USR5453-AP# get bss wlan0bssInternal dtim-period
3
```

6. Set the Fragmentation Threshold

You can specify a fragmentation threshold as a number between 256 and 2,346 to set the frame size threshold in bytes. The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames. If the packet being transmitted is equal to or less than the threshold, fragmentation will not be used. Setting the threshold to the largest value

(2,346 bytes) effectively disables fragmentation.

The following command sets the fragmentation threshold to 2000.

```
USR5453-AP# set radio wlan0 fragmentation-threshold 2000
```

7. Set the RTS Threshold

You can specify an RTS Threshold value between 0 and 2347. The RTS threshold specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, especially one with a lot of clients.

The following command sets the RTS threshold at

```
USR5453-AP# set radio wlan0 rts-threshold 2346
```

8. Configure Basic and Supported Rate Sets

Add a basic rate set	`add basic-rate` *`WirelessInterface`* `rate` *`SomeRate`*
	For example:
	`add basic-rate wlan0 rate 48`

Get current basic rates	`get basic-rate`

Add supported rate	`add supported-rate` *`WirelessInterfaceName`* `rate` *`SomeRate`*
	For example:
	`add supported-rate wlan0 rate 9`

Get current supported rates	`get supported-rate wlan0`

The following command adds "`48`" as a basic rate to `wlan0` (the internal, wireless interface):

```
USR5453-AP# add basic-rate wlan0 rate 48
```

To get the basic rates currently configured for this access point:

```
USR5453-AP# get basic-rate
name   rate
-----------
wlan0  11
wlan0  5.5
wlan0  2
wlan0  1
wlan1  24
wlan1  12
wlan1  6
wlan0  48
```

The following command adds "`9`" as a supported rate to `wlan0` (the internal, wireless interface):

```
USR5453-AP# add supported-rate wlan0 rate 9
```

To get the supported rates currently configured for this access point (using "`wlan0`" as the interface for this example):

```
USR5453-AP# get supported-rate wlan0
rate
----
1
2
5.5
6
11
12
18
24
36
48
54

9
```

Note You can use the "get" command to view current rate sets from the CLI as described in "Get Supported Rate Set" on page 232 and "Get Basic Rate Set" on page 232. However, cannot reconfigure Supported Rate Sets or Basic Rate Sets from the CLI. You must use the Advanced menu's Radio page on the Web User Interface to configure this feature.

MAC Filtering

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in "Understanding Interfaces as Presented in the CLI" on page 190. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

You can control access to Professional Access Point based on Media Access Control (MAC) addresses. Based on how you set the filter, you can *allow* access by only client stations with a listed MAC address or *deny* access by the stations listed.

The Professional Access Point maintains up to five MAC address lists to use as filters. One is the default list, which is used by the Web User Interface. The other four are specific to the access point's wireless network interfaces.

- **Default MAC Address List**

  The default MAC address list is named "default". MAC filtering in the Web User Interface maintains addresses in the default list.

- **Interface-Specific MAC Address Lists**

  Through the CLI, you can maintain a MAC address list for each of the Professional Access Point's wireless interfaces. Unless you initiate an interface's list with the "set" command, the interface uses the list named "default".

Specify an Accept or Deny List
Add MAC Addresses of Client Stations to the Filtering List
Remove MAC Address of a Client Station from the Filtering List
Get Current MAC Filtering Settings

Specify an Accept or Deny List

To set up MAC filtering, you first need to specify which type of list you want to configure, and assign a name to the list.

To set up an **Accept** list:
With this type of list, client stations whose MAC addresses are listed will be allowed access to the access point.
	`set bss` *`interface`* `mac-acl-mode accept-list`
	`set bss` *`interface`* `mac-acl-name` *`list_name`*
	Where *interface* is the wireless network interface for which you want to define a MAC filtering list, and *list_name* is a name that you choose for the list. Valid values for *`interface`* are as follows:
	• wlan0bssInternal
	• wlan0bssGuest
	• wlan0bssVWN1
	• wlan0bssVWN2
	Example:
	`set bss wlan0bssGuest mac-acl-mode accept-list`
	`set bss wlan0bssGuest mac-acl-name Guest`

To set up a **Deny** list:
With this type of list, client stations whose MAC addresses are listed will be denied access to the access point.
	`set bss` *`interface`* `mac-acl-mode deny-list`
	`set bss` *`interface`* `mac-acl-name` *`list_name`*
	Where *interface* is the wireless network interface for which you want to define a MAC filtering list, and *list_name* is a name that you choose for the list. Valid values for *`interface`* are as follows:
	• wlan0bssInternal
	• wlan0bssGuest
	• wlan0bssVWN1
	• wlan0bssVWN2
	Example:
	`set bss wlan0bssInternal mac-acl-mode deny-list`
	`set bss wlan0bssInternal mac-acl-name Internal`

Add MAC Addresses of Client Stations to the Filtering List

To add a MAC address to the list:

```
add mac-acl list_name mac MAC_Address_Of_Client
```

Where *`list_name`* is the name of a MAC filtering list and *`MAC_Address_Of_Client`* is the MAC address of the wireless client that you want to add to the MAC filtering list.

For example, to add 4 new clients to the list named *Internal*:

```
USR5453-AP# add mac-acl Internal mac 00:01:02:03:04:05
USR5453-AP# add mac-acl Internal mac 00:01:02:03:04:06
USR5453-AP# add mac-acl Internal mac 00:01:02:03:04:07
USR5453-AP# add mac-acl Internal mac 00:01:02:03:04:08
```

Remove MAC Address of a Client Station from the Filtering List

To remove a MAC address from the list:

```
remove mac-acl list_name mac MAC_Address_Of_Client
```

Where *list_name* is the name of a MAC filtering list and *MAC_Address_Of_Client* is the MAC address of a wireless client that you want to remove from the MAC filtering list.

For example:

```
USR5453-AP# remove mac-acl Guest mac 00:01:02:03:04:04
```

Get Current MAC Filtering Settings

Mode (Accept or Deny)

The following command shows which type of MAC filtering list is currently configured:

```
get bss interface mac-acl-mode
```

Where *interface* is the wireless network interface for which you want to see the MAC filtering list type.

For example:

```
USR5453-AP# get bss wlan0bssGuest mac-acl-mode
accept-list
```

Client List

The following command shows the clients on the MAC filtering list:

```
USR5453-AP# get mac-acl
name                mac
-----------------------------------
wlan0bssInternal  00:01:02:03:04:05
wlan0bssInternal  00:01:02:03:04:06
wlan0bssInternal  00:01:02:03:04:07
wlan0bssInternal  00:01:02:03:04:08
```

Load Balancing

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 190. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

Load balancing parameters affect the distribution of wireless client connections across multiple access points. Using load balancing, you can prevent scenarios where a single access point in your network shows performance degradation because it is handling a disproportionate share of the wireless traffic. (For an overview of Load Balancing, see “Load Balancing” on page 139.)

The access point provides default settings for load balancing.

The following command examples reconfigure some load balancing settings and get details on the configuration:

```
USR5453-AP# set radio wlan0 load-balance-disassociation-stations 2
USR5453-AP# get radio wlan0 load-balance-disassociation-stations
2
USR5453-AP# set radio wlan0 load-balance-disassociation-utilization 25
USR5453-AP#
USR5453-AP# get radio wlan0 load-balance-disassociation-utilization
25
USR5453-AP# set radio wlan0 load-balance-no-association-utilization 50
USR5453-AP#
USR5453-AP# get radio wlan0 load-balance-no-association-utilization
50
```

Quality of Service

Note Before configuring this feature from the CLI, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 190 The interface name referenced in a command determines if a setting applies to a wired or wireless interface or to the Internal or Guest network.

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like *Voice-over-IP* (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the Professional Access Point.

For a complete conceptual overview of QoS, see“Quality of Service” on page 143.

This table shows a quick view of QOS commands and provides links to detailed examples.

QoS Command	Example
Enable/Disable Wi-Fi Multimedia	set radio wlan0 wme off set radio wlan0 wme on get radio wlan0 wme

QoS Command	Example
About Access Point and Station EDCA Parameters	See "About Access Point and Station EDCA Parameters" on page 240.
Understanding the Queues for Access Point and Station	See "Understanding the Queues for Access Point and Station" on page 240.
Distinguishing between Access Point and Station Settings in QoS Commands	See ""Distinguishing between Access Point and Station Settings in QoS Commands" on page 240.
Get QoS Settings on the Access Point	`get tx-queue`
Get QoS Settings on the Client Station	`get wme-queue`
Set Arbirtation Interframe Spaces (AIFS)	On the access point: `set wme-queue wlan0 with queue` *`Queue_Name`* `to aifs` *`AIFS_Value`* On a client station: `set wme-queue wlan0 with queue` *`Queue_Name`* `to aifs` *`AIFS_Value`* See examples in "Set Arbirtation Interframe Spaces (AIFS)" on page 241
Setting Minimum and Maximum Contention Windows (cwmin, cwmax)	On the access point: `set tx-queue wlan0 with queue` *`Queue_Name`* `to cwmin` *`cwmin_Value`* `cwmax` *`cwmax_Value`* On a client station: `set wme-queue wlan0 with queue` *`Queue_Name`* `to cwmin` *`cwmin_Value`* `cwmax` *`cwmax_Value`* See examples in "Setting Minimum and Maximum Contention Windows (cwmin, cwmax)" on page 242.
Set the Maximum Burst Length (burst) on the Access Point	`set tx-queue wlan0 with queue` *`Queue_Name`* `to burst` *`burst_Value`* See examples in "Set the Maximum Burst Length (burst) on the Access Point" on page 243.
Set Transmission Opportunity Limit (txop-limit) for WMM client stations	`set wme-queue wlan0 with queue` *`Queue_Name`* `to txop-limit` *`txop-limit_Value`* See examples in "Set Transmission Opportunity Limit (txop-limit) for WMM client stations" on page 244.

Enable/Disable Wi-Fi Multimedia

By default, Wi-Fi MultiMedia (WMM) is enabled on the access point. With WMM enabled, QoS settings on the Professional Access Point control both *downstream* traffic flowing from the access point to client station (access point EDCA parameters) and *upstream* traffic flowing from the station to the access point (station EDCA parameters). Enabling WMM essentially activates station-to-access-point QoS control.

Disabling WMM will deactivates QoS control of "station EDCA parameters" on *upstream* traffic flowing from the station to the access point. With WMM disabled, you can still set downstream access-point-to-station QoS parameters but no station-to-access-point QoS parameters.

- To disable WMM:

```
USR5453-AP# set radio wlan0 wme off
USR5453-AP# get radio wlan0 wme
off
```

- To enable WMM:

```
USR5453-AP# set radio wlan0 wme on
USR5453-AP# get radio wlan0 wme
on
```

About Access Point and Station EDCA Parameters

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station (access-point-to-station).

Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point (station-to-access-point). Keep in mind that station-to-access-point parameters apply only when WMM is enabled as described in “Enable/Disable Wi-Fi Multimedia” on page 239.

Understanding the Queues for Access Point and Station

The same types of queues are defined for different kinds of data transmitted from access-point-to-station and station-to-access-point but they are referenced by differently depending on whether you are configuring access point or station parameters.

Data	Access Point	Station
Voice - Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.	data0	vo
Video - High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.	data1	vi
Best Effort - Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.	data2	be
Background - Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).	data3	bk

Distinguishing between Access Point and Station Settings in QoS Commands

Access Point - To get and set QoS settings on the access point, use "**tx-queue**" class name in the command.

Station - To get and set QoS settings on the client station, use the "**wme-queue**" class name in the command.

Get QoS Settings on the Access Point

To view the current QoS settings and queue names for access-point-to-station parameters:

```
USR5453-AP# get tx-queue
name   queue  aifs  cwmin  cwmax  burst
---------------------------------------
wlan0  data0  1     3      7      1.5
wlan0  data1  1     7      15     3.0
wlan0  data2  3     15     63     0
wlan0  data3  7     15     1023   0
```

Get QoS Settings on the Client Station

To view the current QoS settings queue names for station-to-access-point parameters:

```
USR5453-AP# get wme-queue
name   queue  aifs  cwmin  cwmax  txop-limit
--------------------------------------------
wlan0  vo     2     3      7      47
wlan0  vi     2     7      15     94
wlan0  be     3     15     1023   0
wlan0  bk     7     15     1023   0
```

Set Arbirtation Interframe Spaces (AIFS)

Arbitration Inter-Frame Spacing (AIFS) specifies a wait time (in milliseconds) for data frames.

Valid values for AIFS are 1-255.

Set AIFS on the Access Point

To set AIFS on access-point-to-station traffic:

```
set tx-queue wlan0 with queue Queue_Name to aifs AIFS_Value
```

Where *Queue_Name* is the queue on the access point to which you want the setting to apply and *AIFS_Value* is the wait time value you want to specify for AIFS.

For example, this command sets the AIFS wait time on the access point Voice queue (data0) to 13 milliseconds.

```
USR5453-AP# set tx-queue wlan0 with queue data0 to aifs 13
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
USR5453-AP# get tx-queue
name   queue  aifs  cwmin  cwmax  burst
---------------------------------------
wlan0  data0  13    3      7      1.5
wlan0  data1  1     7      15     3.0
wlan0  data2  3     15     63     0
wlan0  data3  7     15     1023   0
```

Set AIFS on the Client Station

To set the AIFS on station-to-access-point traffic:

```
set wme-queue wlan0 with queue Queue_Name to aifs AIFS_Value
```

Where *`Queue_Name`* is the queue on the station to which you want the setting to apply and *`AIFS_Value`* is the wait time value you want to specify for AIFS.

For example, this command sets the AIFS wait time on the station Voice queue (vo) to 14 milliseconds.

```
USR5453-AP# set wme-queue wlan0 with queue vo to aifs 14
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
USR5453-AP# get wme-queue
name    queue  aifs  cwmin  cwmax  txop-limit
--------------------------------------------
wlan0   vo     14    3      7      47
wlan0   vi     2     7      15     94
wlan0   be     3     15     1023   0
wlan0   bk     7     15     1023   0
```

Setting Minimum and Maximum Contention Windows (cwmin, cwmax)

The *Minimum Contention Window* (`cwmin`) sets the upper limit (in milliseconds) of the range from which the initial random backoff wait time is determined. For more details, see “Random Backoff and Minimum / Maximum Contention Windows” on page 146.)

Valid values for the "`cwmin`" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for "`cwmin`" must be lower than the value for "`cwmax`".

The *Maximum Contention Window* (`cwmax`) sets the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. For more details, see “Random Backoff and Minimum / Maximum Contention Windows” on page 146.)

Valid values for the "`cwmax`" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for "`cwmax`" must be higher than the value for "`cwmin`".

Set cwmin and cwmax on the Access Point

To set the Minimum and Maximum Contention Windows (cwmin, cwmax) on access-point-to-station traffic:

```
set tx-queue wlan0 with queue Queue_Name to cwmin cwmin_Value cwmax cwmax_Value
```

Where *`Queue_Name`* is the queue on the access point to which you want the setting to apply and *`cwmin_Value`* and *`cwmax_Value`* are the values (in milliseconds) you want to specify for contention back-off windows.

For example, this command sets the access point Video queue (data1) `cwmin` value to 15 and `cwmax` value to 31.

```
USR5453-AP# set tx-queue wlan0 with queue data1 cwmin 15 cwmax 31
```

View the results of this configuration update (bold in the command output highlights the modified values):

```
USR5453-AP# get tx-queue
name   queue  aifs  cwmin  cwmax  burst
---------------------------------------
wlan0  data0  13    3      7      1.5
wlan0  data1  1     15     31     3.0
wlan0  data2  3     15     63     0
wlan0  data3  7     15     1023   0
```

Set cwmin and cwmax on the Station

To set the Minimum and Maximum Contention Windows (cwmin, cwmax) on station-to-access-point traffic:

```
set wme-queue wlan0 with queue Queue_Name to cwmin cwmin_Value cwmax
cwmax_Value
```

Where `Queue_Name` is the queue on the station to which you want the setting to apply and `cwmin_Value` and `cwmax_Value` are the values (in milliseconds) you want to specify for contention back-off windows.

For example, this command sets the client station Video queue (vi) `cwmin` value to 15 and `cwmax` value to 31.

```
USR5453-AP# set wme-queue wlan0 with queue vi cwmin 7 cwmax 15
```

View the results of this configuration update (bold in the command output highlights the modified values):

```
USR5453-AP# get wme-queue
name   queue  aifs  cwmin  cwmax  txop-limit
--------------------------------------------
wlan0  vo     14    3      7      47
wlan0  vi     2     7      15     94
wlan0  be     3     15     1023   0
wlan0  bk     7     15     1023   0
```

Set the Maximum Burst Length (burst) on the Access Point

The *Maximum Burst Length* (`burst`) specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The `burst` applies only to the access point (access-point-to-station traffic).

Valid values for maximum burst length are 0.0 through 999.9.

To set the maximum burst length on access-point-to-station traffic:

```
set tx-queue wlan0 with queue Queue_Name to burst burst_Value
```

Where `Queue_Name` is the queue on the access point to which you want the setting to apply and `burst_Value` is the wait time value you want to specify for maximum burst length.

For example, this command sets the maximum packet burst length on the access point Best Effort queue (data2) to 0.5.

```
USR5453-AP# set tx-queue wlan0 with queue data2 to burst 0.5
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
USR5453-AP# get tx-queue
name   queue  aifs  cwmin  cwmax  burst
---------------------------------------
wlan0  data0  13    3      7      1.5
wlan0  data1  1     15     31     3.0
wlan0  data2  3     15     63     0.5
wlan0  data3  7     15     1023   0
```

Set Transmission Opportunity Limit (txop-limit) for WMM client stations

The *Transmission Opportunity Limit* (`txop-limit`) specifies an interval of time (in milliseconds) when a WMM client station has the right to initiate transmissions on the wireless network. The `txop-limit` applies only to the client stations (station-to-access-point traffic).

To set the `txop-limit` on station-to-access-point traffic:

```
set wme-queue wlan0 with queue Queue_Name to txop-limit txop-limit_Value
```

Where *`Queue_Name`* is the queue on the station to which you want the setting to apply and *`txop-limit_Value`* is the value you want to specify for the `txop-limit`.

For example, this command sets the `txop-limit` on the station Voice queue (vo) to 49.

```
USR5453-AP# set wme-queue wlan0 with queue vo to txop-limit 49
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
USR5453-AP# get wme-queue
name   queue  aifs  cwmin  cwmax  txop-limit
--------------------------------------------
wlan0  vo     14    3      7      49
wlan0  vi     2     7      15     94
wlan0  be     3     15     1023   0
wlan0  bk     7     15     1023   0
```

Wireless Distribution System

Note Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 190. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface or to the Internal or Guest network.

This table shows a quick view of WDS commands and links to detailed examples.

WDS Command	Example
Configuring a WDS Link	See detailed command example below.
Configuring a WDS Link	`get interface wlan0wds0 detail`

Configuring a WDS Link

To set up a Wireless Distribution System (WDS) link between two wireless networks:

1. Enable the WDS interface (`wlan0wds0`) on the current access point:

   ```
   USR5453-AP# set interface wlan0wds0 status up
   USR5453-AP# set interface wlan0wds0 radio wlan0
   ```

2. Provide the MAC address of the remote access point to which you want to link:

   ```
   USR5453-AP# set interface wlan0wds0 remote-mac MAC_Address_Of_Remote_AP
   ```

   For example:

   ```
   USR5453-AP# set interface wlan0wds0 remote-mac 00:E0:B8:76:1B:14
   ```

Getting Details on a WDS Configuration

Verify the configuration of the WDS link you just configured by getting details on the WDS interface:

```
USR5453-AP# get interface wlan0wds0 detail
Field                Value
-------------------------------------------------------
type                 wds
status               up
description          Wireless Distribution System - Link 1
mac                  00:E0:B8:76:26:08
ip
mask
static-ip
static-mask
rx-bytes             0
rx-packets           0
rx-errors            0
rx-drop              0
rx-fifo              0
```

```
rx-frame          0
rx-compressed     0
rx-multicast      0
tx-bytes          0
tx-packets        0
tx-errors         0
tx-drop           0
tx-fifo           0
tx-colls          0
tx-carrier        0
tx-compressed     0
ssid
bss
security
wpa-personal-key
wep-key-ascii     no
wep-key-length    104
wep-default-key
wep-key-1
wep-key-2
wep-key-3
wep-key-4
vlan-interface
vlan-id
radio             wlan0
remote-mac        00:E0:B8:76:1B:14
wep-key
```

Time Protocol

The *Network Time Protocol* (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock. The timestamp will be used to indicate the date and time of each event in log messages. See http://www.ntp.org for more general information on NTP.

To enable the Network Time Protocol (NTP) server on the access point do the following:

1. Enable the NTP Server

```
set ntp status up
```

2. Provide the Host Name or Address of an NTP Server

```
set ntp server NTP_Server
```

Where *`NTP_Server`* is the host name or IP address of the NTP server you want to use. (USRobotics recommends using the host name rather than the IP address, since IP addresses these change more frequently.)

For example, this command sets the NTP server by host name to "`ntp.instant802.com`"

```
set ntp server ntp.instant802.com
```

3. Get Current Time Protocol Settings

```
USR5453-AP# get ntp detail
```

```
Field   Value
--------------------------
status  up
server  ntp.instant802.com
```

Reboot the Access Point

To reboot the access point, simply type "`reboot`" at the command line:

```
USR5453-AP# reboot
```

Reset the Access Point to Factory Defaults

If you are experiencing extreme problems with the Professional Access Point and have tried all other troubleshooting measures, you can reset the access point. This will restore factory defaults and clear all settings, including settings such as a new password or wireless settings.

The following command resets the access point from the CLI:

```
USR5453-AP# factory-reset
```

Note Keep in mind that the `factory-reset` command resets only the access point you are currently administering; not other access points in the cluster.

For information on the factory default settings, see “Default Settings for the Professional Access Point” on page 16.

Keyboard Shortcuts and Tab Completion Help

The CLI provides keyboard shortcuts to help you navigate the command line and build valid commands, along with "tab completion" hints on available commands that match what you have typed so far. Using the CLI will be easier if you use the tab completion help and learn the keyboard shortcuts.

- Keyboard Shortcuts
- Tab Completion and Help

Keyboard Shortcuts

Action on CLI	Keyboard Shortcut
Move cursor to the beginning of the current line	Ctrl-a Home
Move cursor to the end of the current line	Ctrl-e End
Move cursor back on the current line, one character at a time	Ctrl-b Left Arrow key
Move the cursor forward on the current line, one character at a time	Ctrl-f Right Arrow Key
Start over at a blank command prompt (abandons the input on the current line)	Ctrl-c
Remove one character on the current line.	Ctrl-h
Remove the last word in the current command. (Clears one word at a time from the current command line, always starting with the last word on the line.)	Ctrl-W
Remove characters starting from cursor location to end of the current line. (Clears the current line from the cursor forward.)	Ctrl-k
Remove all characters before the cursor. (Clears the current line from the cursor back to the CLI prompt.)	Ctrl-U
Clear screen but keep current CLI prompt and input in place.	Ctrl-l
Display previous command in history. (Ctrl-p and Ctrl-n let you cycle through a history of all executed commands like Up and Down arrow keys typically do. Up/Down arrow keys also work for this.)	Ctrl-p Up Arrow key
Display next command in history. (Ctrl-p and Ctrl-n let you cycle through a history of all executed commands like Up and Down arrow keys typically do. Up/Down arrow keys also work for this.)	Ctrl-n Down Arrow key
Exit the CLI. (At a blank command prompt, typing Ctrl-d closes the CLI.) (Typing Ctrl-d within command text also removes characters, one at a time, at cursor location like Ctrl-h.)	Ctrl-d

Tab Completion and Help

Help on commands can be requested at the command line interface (CLI) by using the TAB key. (See also “Basic Settings” on page 192.)

Hitting TAB once will attempt to complete the current command.

If multiple completions exist, a beep will sound and no results will be displayed. Enter TAB again to display all available completions.

- **Example 1:** At a blank command line, hit TAB twice to get a list of all commands.

```
USR5453-AP#
add               Add an instance to the running configuration
factory-reset     Reset the system to factory defaults
get               Get field values of the running configuration
reboot            Reboot the system
remove            Remove instances in the running configuration
save-running      Save the running configuration
set               Set field values of the running configuration
```

- **Example 2:** Type "**get** " TAB TAB (including a space after **get**) to see a list of all field options for the **get** command.

```
USR5453-AP# get
association       Associated station
basic-rate        Basic rate of the radio
bridge-port       Bridge ports of bridge interfaces
bss               Basic Service Set of the radio
cluster           Clustering-based configuration settings
cluster-member    Member of a cluster of like-configured access points
config            Configuration settings
detected-ap       Detected access point
dhcp-client       DHCP client settings
dot11             IEEE 802.11
host              Internet host settings
interface         Network interface
ip-route          IP route entry
klog-entry        Kernel log entry
log               Log settings
log-entry         Log entry
mac-acl           MAC address access list item
ntp               Network Time Protocol client
portal            Guest captive portal
radio             Radio
radius-user       RADIUS user
ssh               SSH access to the command line interface
supported-rate    Supported rates of the radio
system            System settings
telnet            Telnet access to the command line interface
tx-queue          Transmission queue parameters
wme-queue         Transmission queue parameters for stations
```

- **Example 3:** Type "**get system v**" TAB. This will result in completion with the only matching field, "**get system version**". (Hit ENTER to get the output results of the command.)

```
USR5453-AP# get system v
USR5453-AP# get system version
```

- **Example 4:** Type "**set**" TAB TAB (including a space after **set**) to get a list of all field options for the **set** command.

```
USR5453-AP# set
bss               Basic Service Set of the radio
cluster           Clustering-based configuration settings
cluster-member    Member of a cluster of like-configured access po
config            Configuration settings
```

```
dhcp-client      DHCP client settings
dot11            IEEE 802.11
host             Internet host settings
interface        Network interface
ip-route         IP route entry
log              Log settings
mac-acl          MAC address access list item
ntp              Network Time Protocol client
portal           Guest captive portal
radio            Radio
radius-user      RADIUS user
ssh              SSH access to the command line interface
system           System settings
telnet           Telnet access to the command line interface
tx-queue         Transmission queue parameters
wme-queue        Transmission queue parameters for stations
```

- **Example 5:** Type "**set mac**" TAB, and the command will complete with the only matching option:

```
USR5453-AP# set mac-acl
```

- **Example 6:** Type "**set cluster**" TAB TAB, and the two matching options are displayed:

```
USR5453-AP# set cluster
cluster          Clustering-based configuration settings
cluster-member   Member of a cluster of like-configured access points
```

- **Example 7:** Type "**add**" TAB TAB (including a space after **add**) to get a list of all field options for the **add** command.

```
USR5453-AP# add
basic-rate       Basic rate of the radio
bridge-port      Bridge ports of bridge interfaces
bss              Basic Service Set of the radio
interface        Network interface
mac-acl          MAC address access list item
radius-user      RADIUS user
supported-rate   Supported rate of the radio
```

- **Example 8:** Type "**remove**" TAB TAB (including a space after **remove**) to get a list of all field options for the **remove** command

```
USR5453-AP# remove
basic-rate       Basic rate of the radio
bridge-port      Bridge ports of bridge interfaces
bss              Basic Service Set of the radio
interface        Network interface
ip-route         IP route entry
mac-acl          MAC address access list item
radius-user      RADIUS user
supported-rate   Supported rates of the radio
```

CLI Class and Field Overview

The following is an introduction to the CLI classes and fields. For a complete reference guide, see “Class and Field Reference” on page 25–253.

Configuration information for the Professional Access Point is represented as a set of classes and objects.

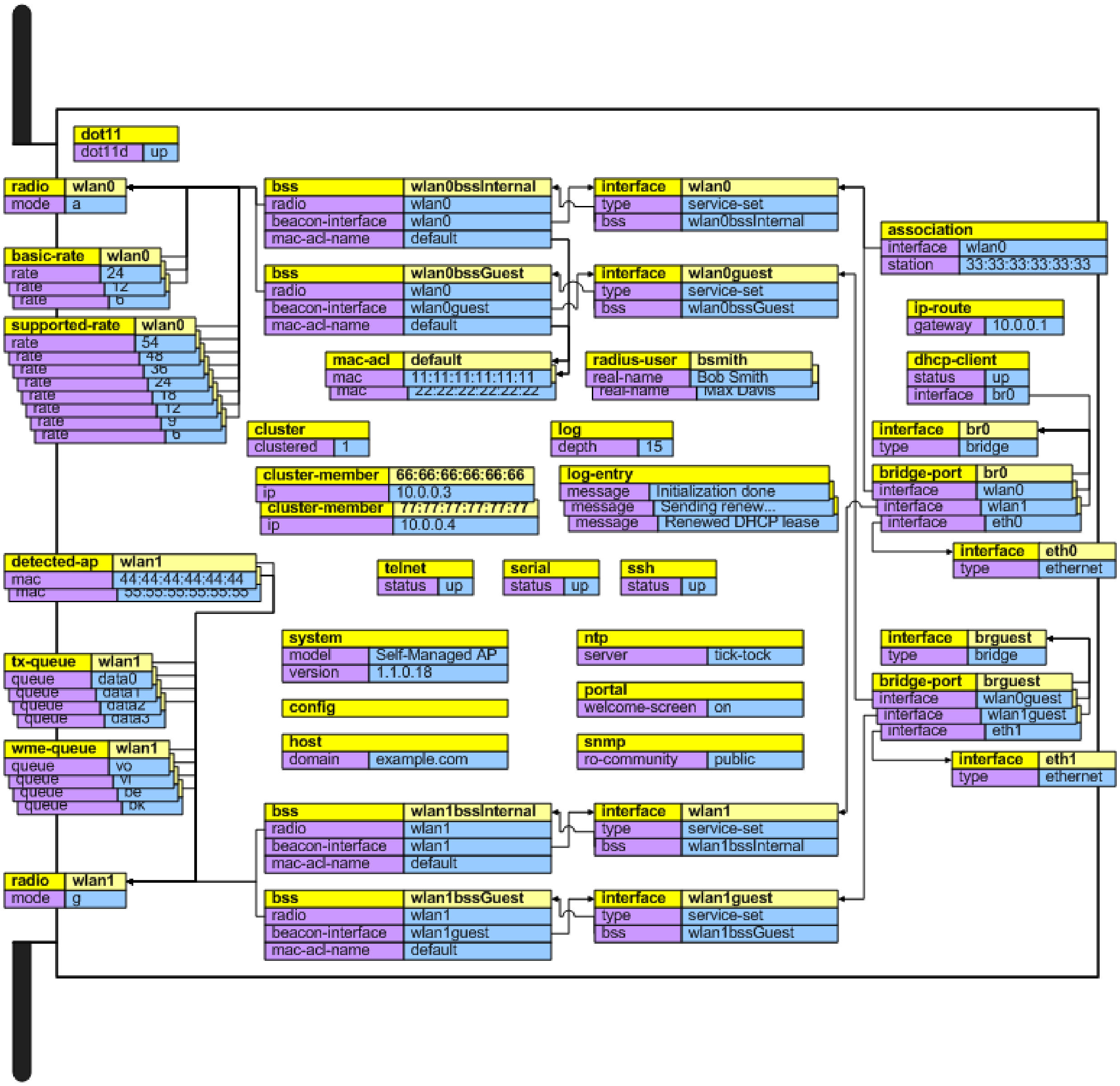
Different kinds of information uses different classes. For example, information about a network interface is represented by the "interface" class, while information about an NTP client is represented by the "ntp" class.

Depending on the type of class, there can be multiple instances of a class. For example, there is one instance of the "interface" class for each network interface that the access point has (Ethernet, radio, and so on), while there is just a singleton instance of the "ntp" class, since an access point needs only a single NTP client. Some classes require their instances to have names to differentiate between them; these are called *named classes*. For example, one interface might have a name of `eth0` to indicate that it is an Ethernet interface, while another interface could have a name of `wlan0` to indicate it is a wireless LAN (WLAN) interface. Instances of singleton classes do not have names, since they only have a single instance. Classes that can have multiple instances but do not have a name are called anonymous classes. Together, singleton and anonymous classes are called unnamed classes. Some classes require their instances to have names, but the multiple instances can have the same name to indicate that they are part of the same group. These are called group classes.

has name? \ # of instances?	one	multiple
no	singleton	anonymous
yes - unique	n/a	unique named
yes - non-unique	n/a	group named

Each class defines a set of fields, that describe the actual information associated with a class. Each instance of a class will have a value for each field that contains the information. For example, the interface class has fields such as "ip" and "mask". For one instance, the `ip` field might have a value of 192.168.1.1 while the `mask` field has a value of 255.255.0.0; another instance might have an `ip` field with a value of 10.0.0.1 and `mask` field with a value of 255.0.0.0.

Figure 10. CLI Class Relationships



Class and Field Reference

Class Index

Class	Description
association	An associated station.
basic-rate	A radio rate.
bridge-port	A port that is a member of a bridge.
bss	A BSS of a radio.
cluster	Stores arbitrary data.
cluster-member	Stores arbitrary data.
config	Config settings.
detected-ap	A detected access point.
dhcp-client	The handler for the DHCP client class.
dot11	802.11 settings (all radios).
host	IP host settings.
interface	A network interface.
ip-route	An IP route.
jvm	Java Virtual Machine.
kickstartd	The handler for the kickstartd class
log	Access point log settings.
log-entry	An entry in the log.
mac-acl	A MAC access list entry.
ntp	Network Time Protocol client settings.
portal	Guest captive portal settings.
radio	A physical radio.
radius-user	A local authentication server user.
serial	The handler for the serial class.
snmp	SNMP server.
ssh	The handler for the ssh class.
supported-rate	A radio rate.
system	System-wide settings.
telnet	The handler for the telnet class.
traphost	An SNMP trap destination host.
tx-queue	A transmission queue.
web-ui	Web user interface settings.
wme-queue	A WME station queue.

association

Persistent: No.
Purpose: An associated station.

Field Index

Field	Description
interface	The interface with which the station is associated.
station	The MAC address of the station.
authenticated	Whether the station is authenticated.
associated	Whether the station is associated.
rx-packets	The number of packets received from the station.
tx-packets	The number of packets transmitted by the station.
rx-bytes	The number of bytes received from the station.
tx-bytes	The number of bytes transmitted by the station.
tx-rate	The transmission rate.
listen-interval	The listen interval.

interface

Purpose	The interface with which the station is associated.
Valid values	Linux network interface name.

station

Purpose	The MAC address of the station.
Valid values	Six colon-separated octets in hexadecimal.

authenticated

Purpose	Whether the station is authenticated.
Valid values	"Yes" or "-".

associated

Purpose	Whether the station is associated.
Valid values	"Yes" or "-".

rx-packets

Purpose	The number of packets received from the station.
Valid values	Positive integer.

tx-packets

Purpose	The number of packets transmitted by the station.
Valid values	Positive integer.

rx-bytes

Purpose	The number of bytes received from the station.
Valid values	Positive integer.

tx-bytes

Purpose	The number of bytes transmitted by the station.
Valid values	Positive integer.

tx-rate

Purpose	The transmission rate.
Valid values	A rate, in 100 kbps.

listen-interval

Purpose	The listen interval.
Valid values	A time, in ms.

basic-rate

Persistent: Yes.
Purpose: A radio rate.
Description: Used to set the rate sets of radios.

Field Index

Field	Description
rate	A radio rate in MBps.

rate

Purpose	A radio rate in MBps. Note that you cannot change an existing rate field; you can only insert or delete the entire instance.
Valid values	Positive integer, or 5.5.

bridge-port

Persistent: Yes.
Purpose: A port that is a member of a bridge.

Field Index

Field	Description
path-cost	The path cost.
priority	The port priority.

path-cost

Purpose	The path cost. Used only when STP is on.
Valid values	1-65535.

priority

Purpose	The port priority. Used only when STP is on.
Valid values	0-255.

bss

Persistent: Yes.
Purpose: A BSS of a radio.
Description: Represents a basic service set.

Field Index

Field	Description
status	Controls whether this is on or off.
description	A human-readable description of the interface.
radio	The radio this is part of.
beacon-interface	The service-set interface to send beacons for.
mac	The MAC address of the interface.
dtim-period	Delivery Traffic Information Map period.
max-stations	Maximum number of stations.
ignore-broadcast-ssid	Do not send SSID in beacons and ignore probe requests.
mac-acl-mode	MAC address Access Control List mode.
mac-acl-name	The name of the mac access control list to use.
radius-accounting	Whether RADIUS accounting is enabled.
radius-ip	The RADIUS server IP address.
radius-key	The RADIUS server shared secret.
open-system-authentication	Whether Open System authentication is permitted.
shared-key-authentication	Whether Shared Key authentication is permitted.
wpa-cipher-tkip	Whether TKIP is permitted as a WPA cipher.
wpa-cipher-ccmp	Whether CCMP is permitted as a WPA cipher.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

description

Purpose A human-readable description of the interface.
Valid values an ASCII string.

radio

Purpose The radio this is part of.
Valid values The name of an existing radio instance.

beacon-interface

Purpose The service-set interface to send beacons for.
Valid values The name of an existing interface instance with type of service-set.

mac

Purpose The MAC address of the interface. Read-only; value is determined by the starting MAC of the radio.
Valid values 6 colon-separated hexadecimal digit pairs.

dtim-period

Purpose Delivery Traffic Information Map period.
Valid values 1-225.

max-stations

Purpose Maximum number of stations.
Valid values 0-2007.

ignore-broadcast-ssid

Purpose Do not send SSID in beacons and ignore probe requests.
Valid values "on" or "off".

mac-acl-mode

Purpose MAC address Access Control List mode.
Valid values "deny-list": deny only stations in list. "accept-list": accept only stations in list. */

mac-acl-name

Purpose The name of the mac access control list to use.
Valid values the name of existing mac-acl instances.

radius-accounting

Purpose Whether RADIUS accounting is enabled. If unset defaults to "off".
Valid values "on" or "off".

radius-ip

Purpose The RADIUS server IP address.
Valid values An IP address.

radius-key

Purpose The RADIUS server shared secret.
Valid values A string.

open-system-authentication

Purpose Whether Open System authentication is permitted.
Valid values "on" or "off".

shared-key-authentication

Purpose Whether Shared Key authentication is permitted.
Valid values "on" or "off".

wpa-cipher-tkip

Purpose Whether TKIP is permitted as a WPA cipher.
Valid values "on" or "off".

wpa-cipher-ccmp

Purpose Whether CCMP is permitted as a WPA cipher.
Valid values "on" or "off".

channel-planner

Persistent: Yes.
Purpose: Stores arbitrary data.

Field Index

This class has the same fields as class cluster-member.

cluster

Persistent: Yes.
Purpose: Stores arbitrary data.

Field Index

This class has the same fields as class cluster-member.

cluster-member

Persistent: Yes.

Purpose: Stores arbitrary data.
Description: No services are restarted.

config

Persistent: Yes.
Purpose: Configuration settings.
Description: Used for configuration fields.

Field Index

Field	Description
startup	Configuration at boot time.
default	Configuration after factory reset.
no-external-updates	Prevent external configuration updates

startup

Purpose Configuration at boot time.
Write-only.
Valid values "default": Reset to factory defaults.
"rescue": Reset to rescue.
"running": Save running configuration.

default

Purpose Configuration after factory reset.
Write-only.
Valid values "rescue": Reset to rescue.
"running": Save running configuration.

no-external-updates

Purpose Prevent external configuration updates.
Valid values "up" or "down".

debug

Persistent: Yes.
Purpose: Access point debug settings.
Description: The debugging parameters of the access point.

Field Index

Field	Description
level	Level of debugging information.
timestamp	Add a timestamp to debugging information.
klevel	Level of kernel debugging information.
olevel	Level of Orchestrator debugging information.
ologhost	Host for Orchestrator to send syslogs to.

level

Purpose Level of debugging information.
Valid values 0-5.

timestamp

Purpose Add a timestamp to debugging information.
Valid values "on" or "off".

klevel

Purpose Level of kernel debugging information.
Valid values 1-8.

olevel

Purpose Level of Orchestrator debugging information.
Valid values 0-7.

ologhost

Purpose Host for Orchestrator to send syslogs to.
Valid values IP address.

detected-ap

Persistent: No.
Purpose: A detected access point.
Description: Represents an access point that has been detected by passive scanning.

Field Index

Field	Description
mac	The MAC address of the AP.
radio	The radio that detected the AP.
beacon-interval	The beacon interval of the AP in kus (1.
capability	The capabilities of the AP.
type	The type of device detected.
privacy	Whether privacy (WEP or WPA) is enabled.
ssid	The SSID of the AP.
wpa	Whether WPA security is enabled.
phy-type	The mode our radio was in when the AP was detected.
band	The RF band the AP was detected in.
channel	The channel of the AP.
rate	The rate of the AP.
signal	The signal of the AP.
erp	The ERP of the AP.
beacons	The number of beacons received from this AP.
last-beacon	The time of the last beacon received from this AP.
supported-rates	The supported rates of the AP.

mac

Purpose The MAC address of the AP.
Valid values Six colon-separated octets in hexadecimal.

radio

Purpose The radio that detected the AP.
Valid values Linux network interface name.

beacon-interval

Purpose The beacon interval of the AP in kus (1.024 ms).
Valid values Positive integer.

capability

Purpose *The capabilities of the AP.*
Valid values C-formatted hexadecmial bitflag.

type

Purpose The type of device detected.
Valid values "AP", "Ad hoc", or "Other".

privacy

Purpose Whether privacy (WEP or WPA) is enabled.
Valid values "On" or "Off".

ssid

Purpose The SSID of the AP.
Valid values String of up to 32 octets.

wpa

Purpose Whether WPA security is enabled.
Valid values "On" or "Off".

phy-type

Purpose The mode your radio was in when the AP was detected.
Valid values 4: IEEE 802.11b.
7: IEEE 802.11g.

band

Purpose The RF band the AP was detected in.
Valid *valu*es "2.4" or "5".

channel

Purpose The channel of the AP.
Valid values Positive integer.

rate

Purpose The rate of the AP.
Valid values Positive integer.

signal

Purpose The signal of the AP.
Valid values Positive integer.

erp

Purpose The ERP of the AP.
Valid values C-formatted hexadecimal number.

beacons

Purpose The number of beacons received from this AP.
Valid values Positive integer.

last-beacon

Purpose The time of the last beacon received from this AP.
Valid values Date and time, in Unix time format.

supported-rates

Purpose The supported rates of the AP.
Valid values Bracketed list of hexadecimal rate codes.

dhcp-client

Persistent: Yes.
Purpose: The handler for the DHCP client class.
Description: Represents a DHCP client.

Field Index

Field	Description
status	Controls whether this is on or off.
interface	The interface to perform DHCP on.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

interface

Purpose The interface to perform DHCP on.
Valid values The name of an existing interface instance. */

dot11

Persistent: Yes.
Purpose: 802.11 settings (all radios).
Description: Represents the wireless functions of the access point.

Field Index

Field	Description
status	Controls whether 802.
debug	The debugging level for 802.
dot11d	Whether AP should enable 802.

status

Purpose Controls whether 802.11 is in use.
Valid values "up" or "down".

debug

Purpose The debugging level for 802.11.
Valid values 0-3.

dot11d

Purpose Whether AP should enable 802.11d
Valid values "up" or "down".

host

Persistent: Yes.
Purpose: IP host settings.
Description: Used for IP host fields.

Field Index

Field	Description
dns-[12]	Domain name servers in use.
domain	Domain name in use.
id	The host name.
static-dns-[12]	Domain name servers to use when not obtained through DHCP.
static-domain	Domain name to use when not obtained through DHCP.
dns-via-dhcp	Whether DNS parameters are obtained through DHCP.

dns-[12]

Purpose	Domain name servers in use.
Valid values	IP address.

domain

Purpose	Domain name in use.
Valid values	DNS domain name.

id

purpose	The host name.
Valid values	DNS domain name.

static-dns-[12]

Purpose	Domain name servers to use when not obtained through DHCP.
Valid values	IP address.

static-domain

Purpose	Domain name to use when not obtained through DHCP.
Valid values	DNS domain name.

dns-via-dhcp

Purpose	Whether DNS parameters are obtained through DHCP.
Valid values	"up" or "down".

interface

Persistent: Yes.
Purpose: A network interface.
Description: Used for per-interface fields.

Field Index

Field	Description
ip	The actual IP address of this interface.
mask	The actual netmask of this interface.
status	Controls whether this is on or off.
type	The type of the interface.
description	A human-readable description of the interface.
mac	The MAC address of the interface.
static-ip	The static IP address of this interface.
static-mask	The static netamsk of this interface.
rx-bytes	Received bytes.
rx-packets	Received packets.
rx-errors	Received packets with errors.
rx-drop	Received packets that were dropped.
rx-fifo	Received packets with FIFO overflows.
rx-frame	Received packets with frame errors.
rx-compressed	Received packets with compression.
rx-multicast	Received packets that were multicast.
tx-bytes	Transmitted bytes.
tx-packets	Transmitted packets.
tx-errors	Transmitted packets with errors.
tx-drop	Transmitted packets that were dropped.
tx-fifo	Transmitted packets with FIFO overflows.
tx-colls	Transmitted packets will collisions.
tx-carrier	Transmitted packets with carrier errors.
tx-compressed	Transmitted packets with compression.

ip

Purpose The actual IP address of this interface. Read-only.
Valid values IP address.

mask

Purpose The actual netmask of this interface.
Read-only.

Valid values Netmask in dotted-decimal notation.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

type

Purpose The type of the interface. Used to determine what additional fields are available. Read-only.
Valid values "service-set", "bridge", "vlan", "wds", "pptp", "pppoe".

description

Purpose A human-readable description of the interface.
Valid values an ASCII string.

mac

Purpose The MAC address of the interface.
Valid values 6 colon-separated hexadecimal digit pairs.

static-ip

Purpose The static IP address of this interface. Used when DHCP is not in use.
Valid values IP address.

static-mask

Purpose The static netamsk of this interface. Used when DHCP is not in use.
Valid values Netmask in dotted-decimal notation.

rx-bytes

Purpose Received bytes.
Valid values Integer.

rx-packets

Purpose Received packets.
Valid values Integer.

rx-errors

Purpose Received packets with errors.
Valid values Integer.

rx-drop

Purpose *Received packets that were dropped*
Valid values Integer.

rx-fifo

Purpose Received packets with FIFO overflows.
Valid values Integer.

rx-frame

Purpose Received packets with frame errors.
Valid values Integer.

rx-compressed

Purpose Received packets with compression.
Valid values Integer.

rx-multicast

Purpose Received packets that were multicast.
Valid values Integer.

tx-bytes

Purpose Transmitted bytes.
Valid values Integer.

tx-packets

Purpose Transmitted packets.
Valid values Integer.

tx-errors

Purpose Transmitted packets with errors.
Valid values Integer.

tx-drop

Purpose Transmitted packets that were dropped.
Valid values Integer.

tx-fifo

Purpose Transmitted packets with FIFO overflows.

Valid values Integer.

tx-colls

Purpose Transmitted packets will collisions.
Valid values Integer.

tx-carrier

Purpose Transmitted packets with carrier errors.
Valid values Integer.

tx-compressed

Purpose Transmitted packets with compression.
Valid values Integer.

ip-route

Persistent: Yes.
Purpose: An IP route.
Description: An IP route.

Field Index

Field	Description
in-use	Whether the route is currently in use.
destination	The destination network prefix.
mask	The mask of the destination network prefix.
gateway	The router by which the destination is reachable.

in-use

Purpose Whether the route is currently in use. Read-only.
Valid values "up" or "down".

destination

Purpose The destination network prefix.
Valid values IP address prefix.

mask

Purpose The mask of the destination network prefix.

Valid values Netmask.

gateway

Purpose The router by which the destination is reachable.
Valid values IP address.

jvm

Persistent: No.
Purpose: Java Virtual Machine.
Description: Represents a JVM.

Field Index

Field	Description
status	Controls whether this is on or off.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

kickstartd

Persistent: No.
Purpose: The handler for the kickstartd class.
Description: Represents a kickstartd process.

log

Persistent: Yes.
Purpose: Access point log settings.
Description: Access point log messages.

Field Index

Field	Description
depth	The number of log entries to keep

depth

Purpose The number of log entries to keep.
Valid values Positive integer.

log-entry

Persistent: No.
Purpose: An entry in the log.
Description: An entry in the log.

Field Index

Field	Description
number	The entry number.
priority	The priority of the log entry.
time	The time of the message.
daemon	The daemon the message is associated with.
message	The message.

number

Purpose The entry number.
Valid values A non-zero integer.

priority

Purpose The priority of the log entry.
Valid values A non-zero integer.

time

Purpose The time of the message.
Valid values A Unix-format time.

daemon

Purpose The daemon the message is associated with.
Valid values String.

message

Purpose The message.
Valid values String.

mac-acl

Persistent: Yes.
Purpose: A MAC access list entry.
Description: Each instance represents a single MAC address. All instances with the same name form a list. This list can be used by BSSes.

Field Index

Field	Description
mac	A MAC address.

mac

Purpose A MAC address.
Valid values 6 colon-separated hexadecimal digit pairs. */

ntp

Persistent: Yes.
Purpose: Network Time Protocol client settings.

Field Index

Field	Description
status	Controls whether this is on or off.
server	The NTP server IP address.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

server

Purpose The NTP server IP address.
Valid values An IP address.

portal

Persistent: Yes.
Purpose: Guest captive portal settings.
Description: Represents a portal. When a portal is run on an interface, traffic entering that interface does not have unconditional access to the AP - they must satisfy some portal requirements, such as clicking through a welcome screen, before access is given.

Field Index

Field	Description
status	Controls whether this is on or off.
welcome-screen	Whether the welcome screen is shown to guest users.
welcome-screen-text	Text to display on the welcome screen.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

welcome-screen

Purpose Whether the welcome screen is shown to guest users.
Valid values "on" or "off".

welcome-screen-text

Purpose Text to display on the welcome screen.
Valid values HTML.

radio

Persistent: Yes.
Purpose: A physical radio.
Description: Represents a physical radio.

Field Index

Field	Description
status	Controls whether the radio is on or off.
description	A human-readable description of the interface.
mac	The MAC address of the radio.
max-bss	The maximum number of BSSes permitted on this radio.
channel-policy	The channel policy of this radio.
mode	The wireless mode of this radio.
super-g	Whether Super G is enabled.
static-channel	The static channel of this radio.
tx-power	The transmit power of this radio.
tx-rx-status	Whether the radio transmits and receives data.
beacon-interval	The beacon interval for this radio in kus (1.
rts-threshold	The size of frames at which RTS/CTS will be used.
fragmentation-threshold	The size of frames at which they will be fragmented.
load-balance-disassociation-utilization	The load that must be exceeded in order for a station to be disassociated.
load-balance-disassociation-stations	The number of associated stations that must be exceeded for a station to be disassociated.
load-balance-no-association-utilization	The load that must be exceeded in order for new stations to be prohibited from associating.
ap-detection	Whether AP detection is performed.
station-isolation	Whether stations are isolated.
wme	Whether WME is enabled.
wme_wifi_noack_test	Mode for Wi-Fi noack test.

status

Purpose	Controls whether the radio is on or off
Valid values	"up" or "down".

description

Purpose	A human-readable description of the interface.
Valid values	an ASCII string.

mac

Purpose The MAC address of the radio. If blank, obtains the MAC address of the radio from hardware. This will be used as the starting MAC address for the BSSes.

Valid values 6 colon-separated hexadecimal digit pairs.

max-bss

Purpose The maximum number of BSSes permitted on this radio. This limits the number of bss instances whose radio field can be this radio's name.

Valid values Positive integers.

channel-policy

Purpose The channel policy of this radio.

Valid values static: Use static-channel.
best: Select the best channel.

mode

Purpose The wireless mode of this radio.

Valid values The Valid values depend on the capabilities of the radio:
b: IEEE 802.11b.
g: IEEE 802.11g.

super-g

Purpose Whether Super G is enabled. If unset defaults to "no".

Valid values "yes" or "no".

static-channel

Purpose The static channel of this radio. Used when channel policy is static.

Valid values Depends on regulatory-domain and mode. All channels are positive integers.

tx-power

Purpose The transmit power of this radio.

Valid values A percentage.

tx-rx-status

Purpose Whether the radio transmits and receives data.

Valid values "up" or "down".

beacon-interval

Purpose The beacon interval for this radio in kus (1.024 ms).

Valid values 20-2000.

rts-threshold

Purpose	The size of frames at which RTS/CTS will be used.
Valid values	0-2347.

fragmentation-threshold

Purpose	The size of frames at which they will be fragmented.
Valid values	256-2346.

load-balance-disassociation-utilization

Purpose	The load that must be exceeded in order for a station to be disassociated. The condition for load-balance-disassociation-stations must also be satisfied, if it is non-zero.
Valid values	A non-zero percentage, or 0 to disable.

load-balance-disassociation-stations

Purpose	The number of associated stations that must be exceeded for a station to be disassociated. The condition for load-balance-disassociation-utilization must also be satisfied, if it is non-zero.
Valid values	1-2007, or 0 to disable.

load-balance-no-association-utilization

Purpose	The load that must be exceeded in order for new stations to be prohibited from associating.
Valid values	A non-zero percentage, or 0 to disable.

ap-detection

Purpose	Whether AP detection is performed. If on, the detected APs will be represented by instances of the detected-ap class.
Valid values	"on" or "off".

station-isolation

Purpose	Whether stations are isolated. If on, then stations on this radio cannot exchange data with other stations on this radio.
Valid values	"on" or "off".

wme

Purpose	Whether WME is enabled. Determines whether wme-queue values will be sent to clients.
Valid values	"on" or "off".

wme_wifi_noack_test

Purpose	Mode for Wi-Fi noack test.

Valid values "on" or "off".

radius-user

Persistent: Yes.
Purpose: A local authentication server user.
Description: Handles username/password and generates password hash

serial

Persistent: Yes.
Purpose: The handler for the serial class.
Description: Represents the serial access to the CLI.

snmp

Persistent: Yes.
Purpose: SNMP server.
Description: Represents a SNMP server.

Field Index

Field	Description
status	Controls whether this is on or off.
ro-community	The read-only community name.
rw-community	The read-write community name.
ip	The IP address of the interface to listen on.
engine-id	The engine identifier.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

ro-community

Purpose The read-only community name.
Valid values String.

rw-community

Purpose The read-write community name.
Valid values String.

ip

Purpose The IP address of the interface to listen on.
Valid values IP address.

engine-id

Purpose The engine identifier.
Valid values A string.

ssh

Persistent: Yes.
Purpose: The handler for the ssh class.
Description: Represents the SSH.

supported-rate

Persistent: Yes.
Purpose: A radio rate.

Field Index

This class has the same fields as class basic-rate.

system

Persistent: Yes.
Purpose: System-wide settings.
Description: Used for system-wide fields.

Field Index

Field	Description
password	The login password.
encrypted-password	The login password, crypted.
password-initialized	Whether the password has been initialized since first boot.
reboot	Reboot the system.

password

Purpose The login password.
Write-only.
Valid values String.

encrypted-password

Purpose The login password, crypted.
Valid values String.

password-initialized

Purpose Whether the password has been initialized since first boot.
Valid values 1, or blank.

reboot

Purpose Reboot the system.
Write-only.
Valid values "yes" to reboot.

telnet

Persistent: Yes.
Purpose: The handler for the telnet class.
Description: Represents Telnet access to the CLI.

traphost

Persistent: Yes.
Purpose: An SNMP trap destination host.
Description: Represents a trapsink, trap2sink and informsink commands in SNMPD configuration file.

Field Index

Field	Description
host	The host to send traps to.
community	The community to send the traps with.
type	The type of traps to send.

host

Purpose The host to send traps to.
Valid values IP address.

community

Purpose The community to send the traps with.
Valid values A string.

type

Purpose The type of traps to send.
Valid values "trapsink", "trap2sink", or "informsink".

tx-queue

Persistent: Yes.
Purpose: A transmission queue.
Description: Represents transmission queue parameters of a radio. The name of the instance must be the same as the name of the radio it represents.

Field Index

Field	Description
queue	The queue.
aifs	Adaptive Inter-Frame Space.
cwmin	Minimum contention window.
cwmax	Maximum contention window.
burst	Maximum burst length.

queue

Purpose The queue.
Valid values "data0", "data1", "data2", "data3", "mgmt", "after_beacon", or "beacon".

aifs

Purpose Adaptive Inter-Frame Space.
Valid values 1-255.

cwmin

Purpose Minimum contention window.
Valid values 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024.

cwmax

Purpose Maximum contention window.
Valid values 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024.

burst

Purpose Maximum burst length.
Valid values 0.0-999.9.

web-ui

Persistent: No.
Purpose: Web user interface settings.
Description: Represents the web user interface of the AP.

Field Index

Field	Description
status	Controls whether this is on or off.

status

Purpose Controls whether this is on or off.
Valid values "up" or "down".

wme-queue

Persistent: Yes.
Purpose: A WME station queue.
Description: Represents queue parameters of a WME station. The name of the instance must be the same as the name of the radio to whose stations it applies to.

Troubleshooting

This part of the Professional Access Point Administrator Guide addresses installation and post-installation troubleshooting issues as follows:

- Installation and Connectivity Troubleshooting
  - The installation procedure does not begin when I insert the Installation CD-ROM.
  - The Professional Access Point Detection Utility does not find the access point.
  - I cannot access the Web User Interface.
  - I need to configure the access point with an operating system other than Windows.
  - My wireless device cannot find the wireless network.
  - I changed the access point settings, and now my wireless device does not establish a wireless connection.
  - I am experiencing poor wireless link quality.
- Configuration Troubleshooting
  - Wireless Distribution System (WDS) Problems and Solutions
  - Cluster Recovery

Installation and Connectivity Troubleshooting

The installation procedure does not begin when I insert the Installation CD-ROM.

Possible Solution:

You may be running a program that interferes with the autolaunch feature of the CD-ROM. Navigate to your CD-ROM drive and launch **Startup.exe**.

The Professional Access Point Detection Utility does not find the

access point.

Possible Solution 1:

1. Ensure that all cables are plugged in firmly, and verify that the access point's power indicator is lighted.

2. In the Detection Utility, click **Back** and then click **Next** to restart the discovery process.

Possible Solution 2:

You can open the access point's Web User Interface without using the Detection Utility by typing the IP address in your Web browser's navigation or address bar. To find the IP address of the access point,

1. Using the configuration program for the networking device to which the access point is connected, view the device's client list.

2. Find the MAC address of the access point in the client list.

3. Note the IP address the corresponds to the MAC address of the access point.

Possible Solution 3:

The access point and the administrator machine may not be connected to the same subnet. Bypass your local area network by connecting the access point directly to the administrator computer, then start the Detection Utility again. If the Detection Utility finds the access point, either the two machines were on different subnets or the problem lies within your LAN.

If you are unable to connect the Access Point and the administrator computer to the same subnet, you can perform Access Point configuration by using the direct connection. For more information about using this method, see "Setting Up and Launching Your Wireless Network" on page 23.

I cannot access the Web User Interface.

Possible Solution 1:

Verify that you are entering the correct IP address in your Web browser.

Possible Solution 2:

Reboot the access point by disconnecting and then reconnecting its power adapter.

Possible Solution 3:

Verify the connection setting of your Web browser, and verify that the HTTP Proxy feature of your Web browser is disabled.

Internet Explorer users:

1. Click **Tools**, click **Internet Options**, and then click the **Connections** tab.

2. Select **Never dial a connection**, and then click the **LAN Settings** button.

3. Clear all the checkboxes and click **OK**.

4. Click **OK** again to apply the connection setting

Netscape Navigator users:

1. Click **Edit**, **Preferences**, and then double-click **Advanced** in the Category window.

2. Click **Proxies**, select **Direct connection to the Internet**, and then click **OK**.

Possible Solution 4:

Note Resetting the access point returns all settings to their factory defaults. You will have to re-enter your configuration settings or restore your configuration backup after resetting the access point.

Reset the access point by using a thin object, such as a paper clip, to press the Reset button until both the LAN and WLAN LEDs turn off briefly.

I need to configure the access point with an operating system other than Windows.

Possible Solution:

You must configure the access point through its Web User Interface as follows:

1. Find the access point's IP address:

    1) Using the configuration program for the networking device to which the access point is connected, view the device's client list.

    2) Find the MAC address of the access point in the client list.

    3) Note the IP address the corresponds to the MAC address of the access point.

2. Launch a Web browser, type the IP address of the access point in the browser's navigation bar, and press Enter.

3. You can now log in and perform access point configuration.

My wireless device cannot find the wireless network.

Possible Solution 1:

Move the wireless device closer to the access point. The device may be out of the access point's range.

Possible Solution 2:

Ensure that the wireless device is set to **Infrastructure** mode and has the following settings in common with the access point:

- SSID, also called **Network Name**.
- Kind of security (for example, WPA)
- Security key value
- 802.11 mode

If you change the settings on the access point, remember to change the settings on your wireless devices also.

Possible Solution 3:

Ensure that the access point is broadcasting its SSID:

1. Open the Web User Interface of the access point.
2. From the **Advanced** menu, select **Security.**
3. Verify that **Broadcast SSID** is set to **Allow.**
4. Click **Update** to save any change.

Possible Solution 4:

If you use MAC filtering on the access point, verify that the MAC address of the client is allowed to access your wireless network:

1. Open the Web User Interface of the access point.
2. From the **Advanced** menu, select **MAC Filtering**.
3. If you selected **Allow only stations in list**, verify that the client's MAC address is included in the Stations List.

   If you selected **Allow any station unless in list**, verify that the client's MAC address is not included in the Stations List.

Possible Solution 5:

Reboot the access point by disconnecting and then reconnecting its power adapter.

Possible Solution 6:

Note

Resetting the access point returns all settings to their factory defaults. You will have to re-enter your configuration settings or restore your configuration backup after resetting the access point.

Reset the access point by using a thin object, such as a paper clip, to press the Reset button press the Reset button until both the LAN and WLAN LEDs turn off briefly.

I changed the access point settings, and now my wireless device does not establish a wireless connection.

Possible Solution:

Ensure that the client device is using the correct Pass phrase and encryption options. If you changed the settings in the configuration of the Professional Access Point, you must also change the settings of every wireless adapter that needs access to the wireless network. The settings of the wireless PC cards, PCI adapters, or USB adapters must match the new settings of the Professional Access Point.

I am experiencing poor wireless link quality.

Possible Solution 1:

Reposition the access point or the wireless device so that environmental factors, such as lead-based paint or concrete walls, do not interfere with your wireless signal.

Possible Solution 2:

Create a wireless connection on a different channel so that electronic devices, such as 2.4 GHz phones, do not interfere with your wireless signal. For more information about changing channels, see “Channel Management” on page 63.

Configuration Troubleshooting

Wireless Distribution System (WDS) Problems and Solutions

If you are having trouble configuring a WDS link, be sure that you have read the notes and cautions in “Configuring WDS Settings” on page 156. These notes are reprinted here for your convenience. The most common problem that administrators encounter with WDS setups is forgetting to set both access points in the link to the same radio channel and IEEE 802.11 mode. That prerequisite, as well as others, is listed in the notes below.

Notes

- The only security mode available on the WDS link is Static WEP, which is not particularly secure. Therefore, USRobotics recommends using WDS to bridge the Guest network only. Do not use WDS to bridge access points on the Internal network unless you are not concerned about the security risk for data traffic on that network.
- When using WDS, be sure to configure WDS settings on *both* access points participating in the WDS link.
- You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.
- Both access points participating in a WDS link must be on the same radio channel and use the same IEEE 802.11 mode. (See “Radio” on page 129 for information on configuring the Radio mode and channel.)
- **Do not create loops** with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. *Spanning Tree Protocol* (STP), which manages path redundancy and prevent unwanted loops, is not available in the Professional Access Point. Keep these rules in mind when working with WDS on the access point:

  Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.

  Do not create backup links.

  If you can trace more than one path between any pair of APs going through any combination of Ethernet or WDS links, you have a loop.

  You can only extend or bridge either the Internal or Guest network but not both.

Cluster Recovery

In cases where the access points in a cluster become out of sync or an access point cannot join or be removed from a cluster, the following methods for cluster recovery are recommended.

Reboot or Reset Access Point

Apply these recovery methods in the order in which they are listed. In all but the last case (stop clustering), you only need to reset or reboot the access point whose configuration is out of synchronization with other cluster members or that cannot join or be removed from the cluster.

1. Reboot the access point by disconnecting and then reconnecting the power cable.

2. Reset the access point through its Web User Interface. To do this, go to `http://`*`IPAddressOfAccessPoint`*, navigate to the Advanced menu’s **Reset Configuration** tab, and click the **Reset** button. (IP addresses for APs are on the Cluster menu’s Access Points page for any cluster member.)

3. Reset the access point by pressing the reset button on the device until both the LAN and WLAN LEDs turn off briefly.

4. In extreme cases, rebooting or resetting may not solve the problem. In these cases, follow the procedure described next in “Stop Clustering and Reset Each Access Point in the Cluster” to recover every

access point on the subnet.

Stop Clustering and Reset Each Access Point in the Cluster

If the previous reboot or reset methods do not solve the problem, do the following to stop clustering and reset all APs.

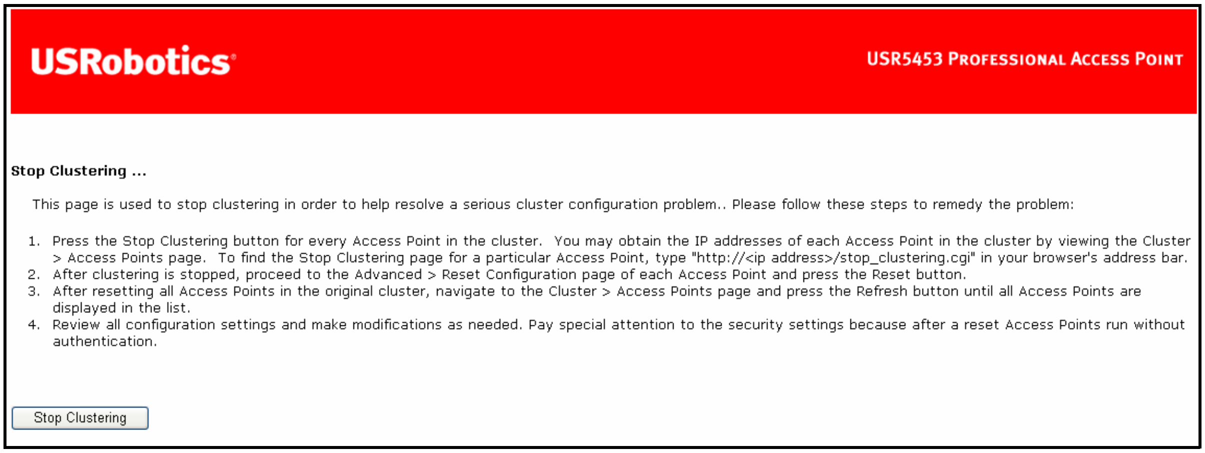
1. Stop clustering on each access point in the cluster.

   To do this, enter the Stop Clustering URL in the address bar of your Web browser as follows:

   `http://`*`IPAddressOfAccessPoint`*`/stop_clustering.cgi`

   Where *`IPAddres0sOfAccessPoint`* is the IP address of the access point that you want to stop clustering. You can find the IP addresses for the cluster members on the Cluster menu's Access Points page for any of the clustered access points. USRobotics recommends making a note of all IP addresses at this point.

   The Stop Clustering page for this access point is displayed.



Stop Clustering ...

This page is used to stop clustering in order to help resolve a serious cluster configuration problem.. Please follow these steps to remedy the problem:

1. Press the Stop Clustering button for every Access Point in the cluster. You may obtain the IP addresses of each Access Point in the cluster by viewing the Cluster > Access Points page. To find the Stop Clustering page for a particular Access Point, type "http://<ip address>/stop_clustering.cgi" in your browser's address bar.
2. After clustering is stopped, proceed to the Advanced > Reset Configuration page of each Access Point and press the Reset button.
3. After resetting all Access Points in the original cluster, navigate to the Cluster > Access Points page and press the Refresh button until all Access Points are displayed in the list.
4. Review all configuration settings and make modifications as needed. Pay special attention to the security settings because after a reset Access Points run without authentication.

   Click **Stop Clustering**.

   Repeat this "stop clustering" step for every access point in the cluster.

Caution Do not proceed to the next step of resetting access points until you have stopped clustering on all access points. Make sure that you first stop clustering on every access point on the subnet, and only then perform the next part of the process of resetting each access point to the factory defaults.

2. Reset each access point.

   To do this, go to the Web User Interface of the access point you want to reset by entering its URL into the address bar of your Web browser:

   `http://`*`IPAddressOfAccessPoint/`*

   Where *`IPAddres0sOfAccessPoint`* is the IP address of the access point you want to reset.

Support Information

If you are having trouble with the configuration or operation of your access point:

1. Refer to the “Troubleshooting” section in this guide.

2. Go to the Support section of the USRobotics Web site at www.usr.com/support/. Many of the most common difficulties that users experience have been addressed in the FAQ and Troubleshooting Web pages for your product. The product number of the Professional Access Point is 5453. You may need to know this to obtain information on the USRobotics Web site.

3. Submit your technical support question using an online form at www.usr.com/emailsupport/.

4. Contact the USRobotics Technical Support Department. To receive assistance, you need your serial number.

Country	Webmail	Voice
U.S.	www.usr.com/emailsupport	(888) 216-2850
Canada	www.usr.com/emailsupport	(888) 216-2850
Austria	www.usr.com/emailsupport/de	07110 900 116
Belgium (Flemish)	www.usr.com/emailsupport/bn	070 23 35 45
Belgium (French)	www.usr.com/emailsupport/be	070 23 35 46
Czech Republic	www.usr.com/emailsupport/cz	
Denmark	www.usr.com/emailsupport/ea	38323011
Finland	www.usr.com/emailsupport/ea	08 0091 3100
France	www.usr.com/emailsupport/fr	0825 070 693
Germany	www.usr.com/emailsupport/de	0180 567 1548
Greece	www.usr.com/emailsupport/gr	
Hungary	www.usr.com/emailsupport/hu	0180 567 1548
Ireland	www.usr.com/emailsupport/uk	1890 252 130
Italy	www.usr.com/emailsupport/it	800 979 266
Luxembourg	www.usr.com/emailsupport/be	342 080 8318
Middle East/Africa	www.usr.com/emailsupport/me	+44 870 844 4546
Netherlands	www.usr.com/emailsupport/bn	0900 202 5857
Norway	www.usr.com/emailsupport/ea	23 16 22 37
Poland	www.usr.com/emailsupport/pl	
Portugal	www.usr.com/emailsupport/pt	21 415 4034
Russia	www.usr.com/emailsupport/ru	8 800 200 20 01
Spain	www.usr.com/emailsupport/es	902 117964
Sweden	www.usr.com/emailsupport/se	08 5016 3205
Switzerland	www.usr.com/emailsupport/de	0848 840 200

Country	Webmail	Voice
Turkey	www.usr.com/emailsupport/tk	0212 444 4 877
UAE	www.usr.com/emailsupport/me	0800 877 63
UK	www.usr.com/emailsupport/uk	0870 844 4546

For current support contact information, go to www.usr.com/support.

Regulatory Information

Declaration of Conformity

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL 60173
U.S.A.

declares that this product conforms to the FCC's specifications:
Part 15, Class B

Operation of this device is subject to the following conditions:
1) this device may not cause harmful electromagnetic interference, and
2) this device must accept any interference received including interference that may cause undesired operations.

This equipment complies with FCC Part 15 for Home and Office use.

Caution to the User: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Detachable Antenna Information

FCC Part 15, Subpart C, Section 15.203 Antenna requirement

USR5453 and USR5453A users: An intentional radiator shall be designed to ensure that no antenna other than that furnished by the responsible party shall be used with the device. The use of a permanently attached antenna or of an antenna that uses a unique coupling to the intentional radiator shall be considered sufficient to comply with the provisions of this section. The manufacturer may design the unit so that a broken antenna can be replaced by the user, but the use of a standard antenna jack or electrical connector is prohibited.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Radio and Television Interference:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy. If this equipment is not installed and used in accordance with the manufacturer's instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

USR declares USR5453 and USR5453A are limited in CH1~11 from 2412 to 2462 MHz by specified firmware controlled in USA.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

UL Listing/CUL Listing:

This information technology equipment is UL Listed and C-UL Listed for both the US and Canadian markets respectively for the uses described in the User Guide. Use this product only with UL Listed Information Technology Equipment (ITE).

For Canadian Users

Industry Canada (IC)

This equipment complies with the Industry Canada Spectrum Management and Telecommunications policy, RSS-210, standard Low Power License-Exempt Radio Communication Devices.

Operation is subject to the following two conditions:

1. This device may cause interference.

2. This device must accept any interference, including interference that may cause undesired operation of the device.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding.

Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Equivalent Isotropic Radiated Power (EIRP) is not more than that required for successful communication.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make electrical ground connections by themselves, but should contact the appropriate inspection authority or an electrician, as appropriate.

CE Compliance

CE0560 ⓘ

Declaration of Conformity

We, U.S. Robotics Corporation of 935 National Parkway, Schaumburg, Illinois, 60173-5157 USA, declare under our sole responsibility that the products, USRobotics Professional Access Point, Models 5453 and 5453A, to which this declaration relates, are in conformity with the following standards and/or other normative documents:

EN300 328
EN301 489-1
EN301 489-17
EN60950-1
EN50392
EN50361

We, U.S. Robotics Corporation, hereby declare the above named product is in compliance and conformity with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The conformity assessment procedure referred to in Article 10 and detailed in Annex IV of Directive 1999/5/EC has been followed.

This equipment is in compliance with the European recommendation 1999/519/ECC, governing the exposure to the electromagnetic radiation.

These products can be used in the following countries: UK, Ireland, Spain, Portugal, Germany, France, Luxembourg, Italy, Switzerland, Austria, Netherlands, Belgium, Norway, Sweden, Denmark, Finland, Czech Republic, Poland, Hungary, and Greece.

An electronic copy of the original CE Declaration of Conformity is available at the U.S. Robotics website: www.usr.com

Regarding IEEE 802.11b/g frequencies, we currently have the following information about restrictions in the European Union (EU) countries:

- Italy

  Please be aware that use of the wireless device is subject to the following Italian regulation:

  1. D.Lgs 1.8.2003, number 259, articles 104 (activities where General Authorization is required) and 105 (free use), for private use;

  2. D.M 28.5.03 and later modifications, for the supplying to public RadioLAN access for networks and telecommunication services

- France

  In France metropolitan, outdoor power is limited to 10mW (EIRP) within 2454MHz – 2483, 5MHz frequency band

In Guyana and Reunion Islands, outdoor use is forbidden within 2400MHz – 2420MHz frequency band

Regulatory Channel Frequency

Channel	Frequency (MHz)	FCC	Canada	ETSI
1	2412	X	X	X
2	2417	X	X	X
3	2422	X	X	X
4	2427	X	X	X
5	2432	X	X	X
6	2437	X	X	X
7	2442	X	X	X
8	2447	X	X	X
9	2452	X	X	X
10	2457	X	X	X
11	2462	X	X	X
12	2467			X
13	2472			X

Operating Channels:	• IEEE 802.11g compliant • 11 channels (US, Canada) • 13 channels (ETSI)

EU Health Protection

This device complies with the European requirements governing exposure to electromagnetic radiation. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. This wireless device is a transmitter/receiver and has been designed and manufactured to comply with the exposure limits recommended by the Council of the European Union and the International Commission on Non-Ionizing Radiation Protection (ICNIRP, 1999) for the entire population. The exposure standard for portable equipment uses the "Specific Absorption Rate" as unit of measure. The maximum SAR value of this wireless device measured in the conformity test is 0.52 W/Kg.

EU Detachable Antenna Information

This USRobotics wireless device has been designed to operate with the antenna included in this package only. Together this device and antenna combination has been tested and approved by a European Agency conforming with the European R&TTE directive 1999/5/EC to meet the radiated power level requirement of 100mW (EIRP). Replacement of this antenna must only be done with an authorized USRobotics component that has been designed and tested with the unit to the requirements of directive 1999/5/EC. Please refer to the U.S. Robotics Web site to get product antenna ordering information.

Go to www.usr.com to see the most recent channel restriction information.

U.S. Robotics Corporation Two (2) Year Limited Warranty

1.0 GENERAL TERMS:

1.1 This Limited Warranty is extended only to the original end-user purchaser (CUSTOMER) and is not transferable.

1.2 No agent, reseller, or business partner of U.S. Robotics Corporation (U.S. ROBOTICS) is authorised to modify the terms of this Limited Warranty on behalf of U.S. ROBOTICS.

1.3 This Limited Warranty expressly excludes any product that has not been purchased as new from U.S. ROBOTICS or its authorised reseller.

1.4 This Limited Warranty is only applicable in the country or territory where the product is intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

1.5 U.S. ROBOTICS warrants to the CUSTOMER that this product will be free from defects in workmanship and materials, under normal use and service, for TWO (2) YEARS from the date of purchase from U.S. ROBOTICS or its authorised reseller.

1.6 U.S. ROBOTICS sole obligation under this warranty shall be, at U.S. ROBOTICS sole discretion, to repair the defective product or part with new or reconditioned parts; or to exchange the defective product or part with a new or reconditioned product or part that is the same or similar; or if neither of the two foregoing options is reasonably available, U.S. ROBOTICS may, at its sole discretion, provide a refund to the CUSTOMER not to exceed the latest published U.S. ROBOTICS recommended retail purchase price of the product, less any applicable service fees. All products or parts that are exchanged for replacement will become the property of U.S. ROBOTICS.

1.7 U.S. ROBOTICS warrants any replacement product or part for NINETY (90) DAYS from the date the product or part is shipped to Customer.

1.8 U.S. ROBOTICS makes no warranty or representation that this product will meet CUSTOMER requirements or work in combination with any hardware or software products provided by third parties.

1.9 U.S. ROBOTICS makes no warranty or representation that the operation of the software products provided with this product will be uninterrupted or error free, or that all defects in software products will be corrected.

1.10 U.S. ROBOTICS shall not be responsible for any software or other CUSTOMER data or information contained in or stored on this product.

2.0 CUSTOMER OBLIGATIONS:

2.1 CUSTOMER assumes full responsibility that this product meets CUSTOMER specifications and requirements.

2.2 CUSTOMER is specifically advised to make a backup copy of all software provided with this product.

2.3 CUSTOMER assumes full responsibility to properly install and configure this product and to ensure proper installation, configuration, operation and compatibility with the operating environment in which this product is to function.

2.4 CUSTOMER must furnish U.S. ROBOTICS a dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) for any warranty claims to be authorised.

3.0 OBTAINING WARRANTY SERVICE:

3.1 CUSTOMER must contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre within the applicable warranty period to obtain warranty service authorisation.

3.2 Customer must provide Product Model Number, Product Serial Number and dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) to obtain warranty service authorisation.

3.3 For information on how to contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre, please see the U.S. ROBOTICS corporate Web site at: www.usr.com

3.4 CUSTOMER should have the following information / items readily available when contacting U.S. ROBOTICS Technical Support:

- Product Model Number
- Product Serial Number
- Dated Proof of Purchase
- CUSTOMER contact name & telephone number
- CUSTOMER Computer Operating System version
- U.S. ROBOTICS Installation CD-ROM
- U.S. ROBOTICS Installation Guide

4.0 WARRANTY REPLACEMENT:

4.1 In the event U.S. ROBOTICS Technical Support or its authorised U.S. ROBOTICS Service Centre determines the product or part has a malfunction or failure attributable directly to faulty workmanship and/or materials; and the product is within the TWO (2) YEAR warranty term; and the CUSTOMER will include a copy of the dated Proof of Purchase (original purchase receipt from U.S. ROBOTICS or its authorised reseller) with the product or part with the returned product or part, then U.S. ROBOTICS will issue CUSTOMER a Return Material Authorisation (RMA) and instructions for the return of the product to the authorised U.S. ROBOTICS Drop Zone.

4.2 Any product or part returned to U.S. ROBOTICS without an RMA issued by U.S. ROBOTICS or its authorised U.S. ROBOTICS Service Centre will be returned.

4.3 CUSTOMER agrees to pay shipping charges to return the product or part to the authorised U.S. ROBOTICS Return Centre; to insure the product or assume the risk of loss or damage which may occur in transit; and to use a shipping container equivalent to the original packaging.

4.4 Responsibility for loss or damage does not transfer to U.S. ROBOTICS until the returned product or part is received as an authorised return at an authorised U.S. ROBOTICS Return Centre.

4.5 Authorised CUSTOMER returns will be unpacked, visually inspected, and matched to the Product Model Number and Product Serial Number for which the RMA was authorised. The enclosed Proof of Purchase will be inspected for date of purchase and place of purchase. U.S. ROBOTICS may deny warranty service if visual inspection of the returned product or part does not match the CUSTOMER supplied information for which the RMA was issued.

4.6 Once a CUSTOMER return has been unpacked, visually inspected, and tested U.S. ROBOTICS will, at its sole discretion, repair or replace, using new or reconditioned product or parts, to whatever extent it deems necessary to restore the product or part to operating condition.

4.7 U.S. ROBOTICS will make reasonable effort to ship repaired or replaced product or part to CUSTOMER, at U.S. ROBOTICS expense, not later than TWENTY ONE (21) DAYS after U.S. ROBOTICS receives the authorised CUSTOMER return at an authorised U.S. ROBOTICS Return Centre.

4.8 U.S. ROBOTICS shall not be liable for any damages caused by delay in delivering or furnishing repaired or replaced product or part.

5.0 LIMITATIONS:

5.1 THIRD-PARTY SOFTWARE: This U.S. ROBOTICS product may include or be bundled with third-party software, the use of which is governed by separate end-user license agreements provided by third-party software vendors. This U.S. ROBOTICS Limited Warranty does not apply to such third-party software. For the applicable warranty refer to the end-user license agreement governing the use of such software.

5.2 DAMAGE DUE TO MISUSE, NEGLECT, NON-COMPLIANCE, IMPROPER INSTALLATION, AND/OR ENVIRONMENTAL FACTORS: To the extent permitted by applicable law, this U.S. ROBOTICS Limited Warranty does not apply to normal wear and tear; damage or loss of data due to interoperability with current and/or future versions of operating system or other current and/or future software and hardware; alterations (by persons other than U.S. ROBOTICS or authorised U.S. ROBOTICS Service Centres); damage caused by operator error or non-compliance with instructions as set out in the user documentation or other accompanying documentation; damage caused by acts of nature such as lightning, storms, floods, fires, and earthquakes, etc. Products evidencing the product serial number has been tampered with or removed; misuse, neglect, and improper handling; damage caused by undue physical, temperature, or electrical stress; counterfeit products; damage or loss of data caused by a computer virus, worm, Trojan horse, or memory content corruption; failures of the product which result from accident, abuse, misuse (including but not limited to improper installation, connection to incorrect voltages, and power points); failures caused by products not supplied by U.S. ROBOTICS; damage cause by moisture, corrosive environments, high voltage surges, shipping, abnormal working conditions; or the use of the product outside the borders of the country or territory intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

5.3 TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. U.S. ROBOTICS NEITHER ASSUMES NOR AUTHORISES ANY OTHER PERSON TO ASSUME FOR IT ANY

OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, WARRANTY, OR USE OF ITS PRODUCTS.

5.4 LIMITATION OF LIABILITY. TO THE FULL EXTENT ALLOWED BY LAW, U.S. ROBOTICS ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF U.S. ROBOTICS OR ITS AUTHORISED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT U.S. ROBOTICS OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

6.0 DISCLAIMER:

Some countries, states, territories or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to CUSTOMER. When the implied warranties are not allowed by law to be excluded in their entirety, they will be limited to the TWO (2) YEAR duration of this written warranty. This warranty gives CUSTOMER specific legal rights, which may vary depending on local law.

7.0 GOVERNING LAW:

This Limited Warranty shall be governed by the laws of the State of Illinois, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL, 60173
U.S.A.

Glossary

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0-9

802

IEEE 802 (IEEE Std. 802-2001) is a family of standards for peer-to-peer communication over a LAN. These technologies use a shared-medium, with information broadcast for all stations to receive. The basic communications capabilities provided are packet-based. The basic unit of transmission is a sequence of data octets (8-bits), which can be of any length within a range that is dependent on the type of LAN.

Included in the 802 family of IEEE standards are definitions of bridging, management, and security protocols.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001) is a standard for passing EAP packets over an 802.11 wireless network using a protocol called *EAP Encapsulation Over LANs* (EAPOL). It establishes a framework that supports multiple authentication methods.

IEEE 802.1x authenticates users not machines.

802.2

IEEE 802.2 (IEEE Std. 802.2.1998) defines the LLC layer for the 802 family of standards.

802.3

IEEE 802.3 (IEEE Std. 802.3-2002) defines the MAC layer for networks that use CSMA/CA. Ethernet is an example of such a network.

802.11

IEEE 802.11 (IEEE Std. 802.11-1999) is a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area. It uses direct sequence spread spectrum (DSSS) in the 2.4 GHz ISM band and supports raw data rates of 1 and 2 Mbps. It was formally adopted in 1997 but has been mostly superseded by 802.11b.

IEEE 802.11 is also used generically to refer to the family of IEEE standards for wireless local area networks.

802.11a

IEEE 802.11a (IEEE Std. 802.11a-1999) is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps.

802.11b

IEEE 802.11b (IEEE Std. 802.11b-1999) is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps.

802.11d

IEEE 802.11d defines standard rules for the operation of IEEE 802.11 wireless LANs in any country without reconfiguration. PHY requirements such as provides frequency hopping tables, acceptable channels, and power levels for each country are provided. Enabling support for IEEE 802.11d on the access point causes the access point to broadcast which country it is operating in as a part of its beacons. Client stations then use this information. This is particularly important for access point operation in the 5GHz IEEE 802.11a bands because use of these frequencies varies a great deal from one country to another.

802.11e

IEEE 802.11e is a developing IEEE standard for MAC enhancements to support QoS. It provides a mechanism to prioritize traffic within 802.11. It defines allowed changes in the Arbitration Interframe Space, a minimum and maximum Contention Window size, and the maximum length (in kμsec) of a burst of data.

IEEE 802.11e is still a draft IEEE standard (most recent version is D5.0, July 2003). A currently available subset of 802.11e is the *Wireless Multimedia Enhancements* (WMM) standard.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) is a standard that defines the inter access point protocol (IAPP) for access points (wireless hubs) in an extended service set (ESS). The standard defines how access points communicate the associations and reassociations of their mobile stations.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003) is a higher speed extension (up to 54 Mbps) to the 802.11b PHY, while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.

802.11i

IEEE 802.11i is a comprehensive IEEE standard for security in a wireless local area network (WLAN) that describes Wi-Fi *Protected Access 2* (WPA2). It defines enhancements to the MAC Layer to counter the some of the weaknesses of WEP. It incorporates stronger encryption techniques than the original Wi-Fi *Protected Access* (WPA), such as Advanced Encryption Standard (AES).

The original WPA, which can be considered a subset of 802.11i, uses *Temporal Key Integrity Protocol* (TKIP) for encryption. WPA2 is backwards-compatible with products that support the original WPA

IEEE 802.11i / WPA2 was finalized and ratified in June of 2004.

802.11k

IEEE 802.11k is a developing IEEE standard for wireless networks (WLANs) that helps auto-manage network Channel selection, client Roaming, and Access Point utilization. 802.11k capable networks will automatically load balance network traffic across APs to improve network performance and prevent under or over-utilization of any one access point. 802.11k will eventually complement the 802.11e quality of service (QoS) standard by ensuring QoS for multimedia over a wireless link.

802.1Q

IEEE 802.1Q is the IEEE standard for *Virtual Local Area Networks* (VLANs) specific to wireless technologies. (See http://www.ieee802.org/1/pages/802.1Q.html.)

The standard addresses the problem of how to break large networks into smaller parts to prevent broadcast and multicast data traffic from consuming more bandwidth than is necessary. 802.11Q also provides for better security between segments of internal networks. The 802.1Q specification provides a standard method for inserting VLAN membership information into Ethernet frames.

A

Access Point

An *access point* acts as a communication hub for the devices on a WLAN, providing a connection or bridge between wireless and wired network devices. It supports a Wireless Networking Framework called Infrastructure Mode.

When one access point is connected to wired network and supports a set of wireless stations, it is referred to as a basic service set (BSS). An extended service set (ESS) is created by combining two or more BSSs.

Ad-hoc Mode

Ad-hoc mode is a Wireless Networking Framework in which stations communicate directly with each other. It is useful for quickly establishing a network in situations where formal infrastructure is not required.

Ad-hoc mode is also referred to as *peer-to-peer mode* or an independent basic service set (IBSS).

AES

The *Advanced Encryption Standard* (AES) is a symmetric 128-bit block data encryption technique developed to replace DES encryption. AES works at multiple network layers simultaneously.

Further information is available on the NIST Web site.

B

Basic Rate Set

The *basic rate set* defines the transmission rates that are mandatory for any station wanting to join this wireless network. All stations must be able to receive data at the rates listed in this set.

Beacon

Beacon frames announce the existence of the wireless local area network and enable stations to establish and maintain communications in an orderly fashion. A beacon frame carries the following information, some of which is optional:

- The *Timestamp* is used by stations to update their local clock, enabling synchronization among all associated stations.
- The *Beacon interval* defines the amount of time between transmitting beacon frames. Before entering power save mode, a station needs the beacon interval to know when to wake up to receive the beacon.
- The *Capability Information* lists requirements of stations that want to join the WLAN. For example, it indicates that all stations must use WEP.
- The *Service Set Identifier* (SSID).
- The Basic Rate Set is a bitmap that lists the rates that the WLAN supports.
- The optional *Parameter Sets* indicates features of the specific signaling methods in use (such as frequency hopping spread spectrum, direct sequence spread spectrum, etc.).
- The optional *Traffic Indication Map* (TIM) identifies stations, using power saving mode, that have data frames queued for them.

Bridge

A connection between two local area networks (LANs) using the same protocol, such as Ethernet or IEEE 802.1x.

Broadcast

A *Broadcast* sends the same message at the same time to everyone. In wireless networks, broadcast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames to all client stations on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Unicast and Multicast.

Broadcast Address

See IP Address.

BSS

A *basic service set* (BSS) is an Infrastructure Mode Wireless Networking Framework with a single access point. Also see extended service set (ESS) and independent basic service set (IBSS).

BSSID

In Infrastructure Mode, the *Basic Service Set Identifier* (BSSID) is the 48-bit MAC address of the wireless interface of the Access Point.

C

CCMP

Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for 802.11i that uses AES. It employs a *CCM* mode of operation, combining the Cipher Block Chaining Counter mode (CBC-CTR) and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

AES-CCMP requires a hardware coprocessor to operate.

CGI

The *Common Gateway Interface* (CGI) is a standard for running external programs from an HTTP server. It specifies how to pass arguments to the executing program as part of the HTTP request. It may also define a set of environment variables.

A CGI program is a common way for an HTTP server to interact dynamically with users. For example, an HTML page containing a form can use a CGI program to process the form data after it is submitted.

Channel

The *Channel* defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each 802.11 standard offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC), the European Telecommunications Standards Institute (ETSI), the Korean Communications Commission, or the Telecom Engineering Center (TELEC).

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a low-level network arbitration/contention protocol. A station listens to the media and attempts to transmit a packet when the channel is quiet. When it detects that the channel is idle, the station transmits the packet. If it detects that the channel is busy, the station waits a random amount of time and then attempts to access the media again.

CSMA/CA is the basis of the IEEE 802.11e Distributed Control Function (DCF). See also RTS and CTS.

The CSMA/CA protocol used by 802.11 networks is a variation on CSMA/CD (used by Ethernet networks). In CSMA/CD the emphasis is on collision *detection* whereas with CSMA/CA the emphasis is on collision *avoidance*.

CTS

A *clear to send* (CTS) message is a signal sent by an IEEE 802.11 client station in response to an *request to send* (RTS) message. The CTS message indicates that the channel is clear for the sender of the RTS message to begin data transfer. The other stations will wait to keep the air waves clear. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS.)

D

DCF

The *Distribution Control Function* is a component of the IEEE 802.11e Quality of Service (QoS) technology standard. The DCF coordinates channel access among multiple stations on a wireless network by controlling wait times for channel access. Wait times are determined by a random backoff timer which is configurable by defining minimum and maximum contention windows. See also EDCF.

DHCP

The *Dynamic Host Configuration Protocol* (DHCP) is a protocol specifying how a central server can dynamically provide network configuration information to clients. A DHCP server offers a lease (for a pre-configured period of time—see Lease Time) to the client system. The information supplied includes the client's IP addresses and netmask plus the address of its DNS servers and Gateway.

DNS

The *Domain Name Service* (DNS) is a general-purpose query service used for translating *fully-qualified names* into Internet addresses. A fully-qualified name consists of the hostname of a system plus its domain name. For example, `www` is the host name of a Web server and `www.usr.com` is the fully-qualified name of that server. DNS translates the domain name `www.usr.com` to an IP address, for example `66.93.138.219`.

A *domain name* identifies one or more IP addresses. Conversely, an IP address may map to more than one domain name.

A domain name has a suffix that indicates which *top level domain* (TLD) it belongs to. Every country has its own top-level domain, for example `.de` for Germany, `.fr` for France, `.jp` for Japan, `.tw` for Taiwan, `.uk` for the United Kingdom, `.us` for the U.S.A., and so on. There are also `.com` for commercial bodies, `.edu` for educational institutions, `.net` for network operators, and `.org` for other organizations as well as `.gov` for the U. S. government and `.mil` for its armed services.

DOM

The *Document Object Model* (DOM) is an interface that allows programs and scripts to dynamically access and update the content, structure, and style of documents. The DOM allows you to model the objects in an HTML or XML document (text, links, , tables), defining the attributes of each object and how they can be manipulated.

Further details about the DOM can be found at the W3C.

DTIM

The *Delivery Traffic Information Map* (DTIM) message is an element included in some Beacon frames. It indicates which stations, currently sleeping in low-power mode, have data buffered on the Access Point awaiting pick-up. Part of the DTIM message indicates how frequently stations must check for buffered data.

Dynamic IP Address

See IP Address.

E

EAP

The *Extensible Authentication Protocol* (EAP) is an authentication protocol that supports multiple methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards.

Variations on EAP include EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS, and EAP Tunnelled TLS (EAP-TTLS).

EDCF

Enhanced Distribution Control Function is an extension of DCF. EDCF, a component of the IEEE Wireless Multimedia (WMM) standard, provides prioritized access to the wireless medium

ESS

An *extended service set* (ESS) is an Infrastructure Mode Wireless Networking Framework with multiple access points, forming a single subnetwork that can support more clients than a basic service set (BSS). Each access point supports a number of wireless stations, providing broader wireless coverage for a large space, for example, an office.

Ethernet

Ethernet is a local-area network (LAN) architecture supporting data transfer rates of 10 Mbps to 1 Gbps. The Ethernet specification is the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. It uses the CSMA/CA access method to handle simultaneous demands.

Ethernet supports data rates of 10 Mbps, *Fast Ethernet* supports 100 Mbps, and *Gigabit Ethernet* supports 1 Gbps. Its cables are classified as "*X*base*Y*", where *X* is the data rate in Mbps and *Y* is the category of cabling. The original cable was *10base5* (Thicknet or "Yellow Cable"). Some others are *10base2* (Cheapernet), *10baseT* (Twisted Pair), and *100baseT* (Fast Ethernet). The latter two are commonly supplied using *CAT5* cabling with *RJ-45* connectors. There is also *1000baseT* (Gigabit Ethernet).

ERP

The *Extended Rate Protocol* refers to the protocol used by IEEE 802.11g stations (over 20 Mbps transmission rates at 2.4GHz) when paired with Orthogonal Frequency Division Multiplexing (OFDM). Built into ERP and the IEEE 802.11g standard is a scheme for effective interoperability of IEEE 802.11g stations with IEEE 802.11b nodes on the same channel.

Legacy IEEE 802.11b devices cannot detect the ERP-OFDM signals used by IEEE 802.11g stations, and this can result in collisions between data frames from IEEE 802.11b and IEEE 802.11g stations.

If there is a mix of 802.11b and 802.11g nodes on the same channel, the IEEE 802.11g stations detect this via an ERP flag on the access point and enable *request to send* (RTS) and *clear to send* (CTS) protection before sending data.

See also CSMA/CA protocol.

F

Frame

A *Frame* consists of a discrete portion of data along with descriptive meta-information packaged for transmission on a wireless network. Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection. A Frame is similar in concept to a Packet, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).

G

Gateway

A *gateway* is a network node that serves as an entrance to another network. A gateway also often provides a proxy server and a firewall. It is associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch or bridge, which provides the actual path for the packet in and out of the gateway.

Before a host on a LAN can access the Internet, it needs to know the address of its *default gateway*.

H

HTML

The *Hypertext Markup Language* (HTML) defines the structure of a document on the World Wide Web. It uses tags and attributes to hint about a layout for the document.

An HTML document starts with an `<html>` tag and ends with a `</html>` tag. A properly formatted document also contains a `<head>`...`</head>` section, which contains the metadata to define the document, and a `<body>`...`</body>` section, which contains its content. Its markup is derived from the *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986.

HTML documents are sent from server to browser via HTTP. Also see XML.

HTTP

The *Hypertext Transfer Protocol* (HTTP) defines how messages are formatted and transmitted on the World Wide Web. An HTTP message consists of a URL and a command (`GET`, `HEAD`, `POST`, etc.), a request followed by a response.

I

IAPP

The *Inter Access Point Protocol* (IAPP) is an IEEE standard (802.11f) that defines communication between the access points in a "distribution system." This includes the exchange of information about mobile stations and the maintenance of bridge forwarding tables, plus securing the communications between access points.

IBSS

An *independent basic service set* (IBSS) is an Ad-hoc Mode Wireless Networking Framework in which stations communicate directly with each other.

IEEE

The Institute of Electrical and Electronic Engineers (IEEE) is an international standards body that develops and establishes industry standards for a broad range of technologies, including the 802 family of networking and wireless standards. (See 802, 802.1x, 802.11, 802.11a, 802.11b, 802.11e, 802.11f, 802.11g, and 802.11i.)

For more information about IEEE task groups and standards, see http://standards.ieee.org/.

Infrastructure Mode

Infrastructure Mode is a Wireless Networking Framework in which wireless stations communicate with each other by first going through an Access Point. In this mode, the wireless stations can communicate with each other or can communicate with hosts on a wired network. The access point is connected to a wired network and supports a set of wireless stations.

An infrastructure mode framework can be provided by a single access point (BSS) or a number of access points (ESS).

Intrusion Detection

The *Intrusion Detection System* (IDS) inspects all inbound network activity and reports suspicious patterns that may indicate a network or system attack from someone attempting to break into the system. It reports access attempts using unsupported or known insecure protocols.

IP

The *Internet Protocol* (IP) specifies the format of packets, also called datagrams, and the addressing scheme. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and reassembly. It is combined with higher-level protocols, such as TCP or UDP, to establish the virtual connection between destination and source.

The current version of IP is *IPv4*. A new version, called IPv6 or IPng, is under development. IPv6 is an attempt to solve the shortage of IP addresses.

IP Address

Systems are defined by their *IP address*, a four-byte (octet) number uniquely defining each host on the Internet. It is usually shown in the form `192.168.2.254`. This is called dotted-decimal notation.

An IP address is partitioned into two portions: the network prefix and a host number on that network. A Subnet Mask is used to define the portions. There are two special host numbers:

- The Network Address consists of a host number that is all zeroes (for example, `192.168.2.0`).
- The Broadcast Address consists of a host number that is all ones (for example, `192.168.2.255`).

There are a finite number of IP addresses that can exist. Therefore, a local area network typically uses one of the IANA-designated address ranges for use in private networks. These address ranges are:

`10.0.0.0` to `10.255.255.255`
`172.16.0.0` to `172.31.255.255`
`192.168.0.0` to `192.168.255.255`

A Dynamic IP Address is an IP address that is automatically assigned to a host by a DHCP server or similar mechanism. It is called dynamic because you may be assigned a different IP address each time you establish a connection.

A Static IP Address is an IP address that is hard-wired for a specific host. A static address is usually required for any host that is running a server, for example, a Web server.

IPSec

IP Security (IPSec) is a set of protocols to support the secure exchange of packets at the IP layer. It uses shared public keys. There are two encryption modes: Transport and Tunnel.

- *Transport* mode encrypts only the data portion (payload) of each packet, but leaves the headers untouched.

- The more secure *Tunnel* mode encrypts both the header and the payload.

ISP

An *Internet Service Provider* (ISP) is a company that provides access to the Internet to individuals and companies. It may provide related services such as virtual hosting, network consulting, Web design, etc.

J

Jitter

Jitter is the difference between the latency (or delay) in packet transmission from one node to another across a network. If packets are not transmitted at a consistent rate (including Latency), QoS for some types of data can be affected. For example, inconsistent transmission rates can cause distortion in VoIP and streaming media. QoS is designed to reduce jitter along with other factors that can impact network performance.

L

Latency

Latency, also known as *delay*, is the amount of time it takes to transmit a Packet from sender to receiver. Latency can occur when data is transmitted from the access point to a client and vice versa. It can also occur when data is transmitted from access point to the Internet and vice versa. Latency is caused by *fixed network* factors such as the time it takes to encode and decode a packet, and also by *variable network* factors such as a busy or overloaded network. QoS features are designed to minimize latency for high priority network traffic.

LAN

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, the computers in your home that you want to network together or a couple of floors in a building. A LAN connects multiple computers and other network devices such as storage and printers. Ethernet is the most common technology implementing a LAN.

Wireless Ethernet (802.11) is another very popular LAN technology (also see WLAN).

LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a protocol for accessing on-line directory services. It is used to provide an authentication mechanism. It is based on the X.500 standard, but less complex.

Lease Time

The *Lease Time* specifies the period of time the DHCP Server gives its clients an IP Address and other required information. When the lease expires, the client must request a new lease. If the lease is set to a short span, you can update your network information and propagate the information provided to the clients in a timely manner.

LLC

The *Logical Link Control* (LLC) layer controls frame synchronization, flow control, and error checking. It is a higher level protocol over the PHY layer, working in conjunction with the MAC layer.

M

MAC

The *Media Access Control* (MAC) layer handles moving data packets between NICs across a shared channel. It is a higher level protocol over the PHY layer. It provides an arbitration mechanism in an attempt to prevent signals from colliding.

It uses a hardware address, known as the *MAC address*, that uniquely identifies each node of a network. IEEE 802 network devices share a common 48-bit MAC address format, displayed as a string of twelve (12) hexadecimal digits separated by colons, for example `FE:DC:BA:09:87:65`.

MIB

Management Information Base (MIB) is a database of objects used for network management. SNMP agents along with other SNMP tools can be used to monitor any network device defined in the MIB.

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) provides authentication for PPP connections between a Windows-based computer and an Access Point or other network access device.

MTU

The *Maximum Transmission Unit* is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are fragmented into smaller packets before being sent.

Multicast

A *Multicast* sends the same message to a select group of recipients. Sending an e-mail message to a mailing list is an example of multicasting. In wireless networks, multicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames to a specified set of client stations (MAC addresses) on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Unicast and Broadcast.

N

NAT

Network Address Translation is an Internet standard that masks the internal IP addresses being used in a LAN. A NAT server running on a gateway maintains a translation table that maps all internal IP addresses in outbound requests to its own address and converts all inbound requests to the correct internal host.

NAT serves three main purposes: it provides security by obscurity by hiding internal IP addresses, enables the use of a wide range of internal IP addresses without fear of conflict with the addresses used by other organizations, and it allows the use of a single Internet connection.

Network Address

See IP Address.

NIC

A *Network Interface Card* is an adapter or expansion board inserted into a computer to provide a physical connection to a network. Most NICs are designed for a particular type of network, protocol, and media, for example, Ethernet or wireless.

NTP

The *Network Time Protocol* assures accurate synchronization of the system clocks in a network of computers. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. An NTP client sends periodic time requests to servers, using the returned time stamp to adjust its clock.

O

OSI

The *Open Systems Interconnection* (OSI) reference model is a framework for network design. The OSI model consists of seven layers:

- Layer 1, the Physical layer, identifies the physical medium used for communication between nodes. In the case of wireless networks, the physical medium is air, and radio frequency (RF) waves are a components of the physical layer.

- Layer 2, the Data-Link layer, defines how data for transmission will be structured and formatted, along with low-level protocols for communication and addressing. For example, protocols such as CSMA/CA and components like MAC addresses, and Frames are all defined and dealt with as a part of the Data-Link layer.

- Layer 3, the Network layer, defines the how to determine the best path for information traversing the network. Packets and logical IP Addresses operate on the network layer.

- Layer 4, the Transport layer, defines connection oriented protocols such as TCP and UDP.

- Layer 5, the Session layer, defines protocols for initiating, maintaining, and ending communication and transactions across the network. Some common examples of protocols that operate on this layer are network file system (NFS) and structured query language (SQL). Also part of this layer are communication flows like single mode (device sends information bulk), half-duplex mode (devices take turns transmitting information in bulk), and full-duplex mode (interactive, where devices transmit and receive simultaneously).

- Layer 6, the Presentation layer, defines how information is presented to the application. It includes meta-information about how to encrypt/decrypt and compress/decompress the data. JPEG and TIFF file formats are examples of protocols at this layer.

- Layer 7, the Application layer, includes protocols like hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

P

Packet

Data and media are transmitted among nodes on a network in the form of *packets*. Data and multimedia content is divided up and packaged into *packets*. A packet includes a small chunk of the content to be sent along with its destination address and sender address. Packets are pushed out onto the network and inspected by each node. The node to which it is addressed is the ultimate recipient.

Packet Loss

Packet Loss describes the percentage of packets transmitted over the network that did not reach their intended destination. A 0 percent package loss indicates no packets were lost in transmission. QoS features are designed to minimize packet loss.

PHY

The Physical Layer (PHY) is the lowest layer in the network layer model (see OSI). The Physical Layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a medium, including defining cables, NICs, and physical aspects.

Ethernet and the 802.11 family are protocols with physical layer components.

PID

The *Process Identifier* (PID) is an integer used by Linux to uniquely identify a process. A PID is returned by the `fork()` system call. It can be used by `wait()` or `kill()` to perform actions on the given process.

Port Forwarding

Port Forwarding creates a ‘tunnel’ through a firewall, allowing users on the Internet access to a service running on one of the computers on your LAN, for example, a Web server, an FTP or SSH server, or other services. From the outside user’s point of view, it looks like the service is running on the firewall.

PPP

The *Point-to-Point Protocol* is a standard for transmitting network layer datagrams (IP packets) over serial point-to-point links. PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on a LAN to the Internet through a common broadband medium, such as a single DSL or cable modem line.

PPtP

Point-to-Point Tunneling Protocol (PPtP) is a technology for creating a *Virtual Private Network* (VPN) within the *Point-to-Point Protocol* (PPP). It is used to ensure that data transmitted from one VPN node to another are secure.

Proxy

A *proxy* is server located between a client application and a real server. It intercepts requests, attempting to fulfill them itself. If it cannot, it forwards them to the real server. Proxy servers have two main purposes: improve performance by spreading requests over several machines and filter requests to prevent access to specific servers or services.

PSK

Pre-Shared Key (PSK), see Shared Key.

Public Key

A *public key* is used in public key cryptography to encrypt a message which can only be decrypted with the recipient's private or secret key. Public key encryption is also called asymmetric encryption, because it uses two keys, or Diffie-Hellman encryption. Also see Shared Key.

Q

QoS

Quality of Service (QoS) defines the performance properties of a network service, including guaranteed throughput, transit delay, and priority queues. QoS is designed to minimize Latency, Jitter, Packet Loss, and network congestion, and provide a way of allocating dedicated bandwidth for high priority network traffic.

The IEEE standard for implementing QoS on wireless networks is currently in-work by the 802.11e task group. A subset of 802.11e features is described in the WMM specification.

R

RADIUS

The *Remote Authentication Dial-In User Service* (RADIUS) provides an authentication and accounting system. It is a popular authentication mechanism for many ISPs.

RC4

A symmetric stream cipher provided by RSA Security. It is a variable key-size stream cipher with byte-oriented operations. It allows keys up to 2048 bits in length.

Roaming

In IEEE 802.11 parlance, *roaming clients* are mobile client stations or devices on a wireless network (WLAN) that require use of more than one a as they move out of and into range of different base station service areas. IEEE 802.11f defines a standard by which APs can communicate information about client associations and disassociations in support of roaming clients.

Router

A *router* is a network device which forwards packets between networks. It is connected to at least two networks, commonly between two local area networks (LANs) or between a LAN and a wide-area network (WAN), for example, the Internet. Routers are located at gateways—places where two or more networks connect.

A router uses the content of headers and its tables to determine the best path for forwarding a packet. It uses protocols such as the Internet Control Message Protocol (ICMP), Routing Information Protocol (RIP), and Internet Router Discovery Protocol (IRDP) to communicate with other routers to configure the best route between any two hosts. The router performs little filtering of data it passes.

RSSI

The *Received Signal Strength Indication* (RSSI) an 802.1x value that calculates voltage relative to the received signal strength. RSSI is one of several ways of measuring and indicating *radio frequency* (RF) signal strength. Signal strength can also be measured in mW (milliwatts), dBms (decibel milliwatts), and a percentage value.

RTP

Real-Time Transport Protocol (RTP) is an Internet protocol for transmitting real-time data like audio and video. It does not guarantee delivery but provides support mechanisms for the sending and receiving applications to enable streaming data. RTP typically runs on top of the UDP protocol, but can support other transport protocols as well.

RTS

A *request to send* (RTS) message is a signal sent by a client station to the access point, asking permission to send a data packet and to prevent other wireless client stations from grabbing the radio waves. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS Threshold and CTS.)

RTS Threshold

The *RTS threshold* specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, and is especially useful for performance tuning on an access point with a many clients.

S

Shared Key

A *shared key* is used in conventional encryption where one key is used both for encryption and decryption. It is also called *secret-key* or *symmetric-key* encryption.

Also see Public Key.

SNMP

The *Simple Network Management Protocol* (SNMP) was developed to manage and monitor nodes on a network. It is part of the TCP/IP protocol suite.

SNMP consists of managed devices and their agents, and a management system. The agents store data about their devices in *Management Information Bases* (MIBs) and return this data to the SNMP management system when requested.

SSID

The *Service Set Identifier* (SSID) is a thirty-two character alphanumeric key that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Static IP Address

See IP Address.

STP

The *Spanning Tree Protocol* (STP) an IEEE 802.1 standard protocol (related to network management) for MAC bridges that manages path redundancy and prevents undesirable loops in the network created by multiple active paths between client stations. Loops occur when there multiple routes between access points. STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN

Subnet Mask

A *Subnet Mask* is a number that defines which part of an IP address is the network address and which part is a host address on the network. It is shown in dotted-decimal notation (for example, a 24-bit mask is shown as `255.255.255.0`) or as a number appended to the IP address (for example, `192.168.2.0/24`).

The subnet mask allows a router to quickly determine if an IP address is local or needs to be forwarded by performing a bitwise AND operation on the mask and the IP address. For example, if an IP address is `192.168.2.128` and the netmask is `255.255.255.0`, the resulting Network address is `192.168.2.0`.

The bitwise AND operator compares two bits and assigns 1 to the result only if both bits are 1. The following table shows the details of the netmask:

IP address	`192.168.2.128`	`11000000 10101000 00000010 10000000`
Netmask	`255.255.255.0`	`11111111 11111111 11111111 00000000`
Resulting network address	`192.168.2.0`	`11000000 10101000 00000010 00000000`

Supported Rate Set

The *supported rate set* defines the transmission rates that are available on this wireless network. A station may be able to receive data at any of the rates listed in this set. All stations must be able to receive data at the rates listed in the Basic Rate Set.

T

TCP

The *Transmission Control Protocol* (TCP) is built on top of Internet Protocol (IP). It adds reliable communication (guarantees delivery of data), flow-control, multiplexing (more than one simultaneous connection), and connection-oriented transmission (requires the receiver of a packet to acknowledge receipt to the sender). It also guarantees that packets will be delivered in the same order in which they were sent.

TCP/IP

The Internet and most local area networks are defined by a group of protocols. The most important of these is the *Transmission Control Protocol over Internet Protocol* (TCP/IP), the de facto standard protocols. TCP/IP was originally developed by Defense Advanced Research Projects Agency (DARPA, also known as ARPA, an agency of the US Department of Defense).

Although TCP and IP are two specific protocols, TCP/IP is often used to refer to the entire protocol suite based upon these, including ICMP, ARP, UDP, and others, as well as applications that run upon these protocols, such as telnet, FTP, etc.

TKIP

The *Temporal Key Integrity Protocol* (TKIP) provides an extended 48-bit initialization vector, per-packet key construction and distribution, a Message Integrity Code (MIC, sometimes called "Michael"), and a rekeying mechanism. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission. It is an important component of the WPA and 802.11i security mechanisms.

ToS

TCP/IP packet headers include a 3-to-5 bit Type *of Service* (ToS) field set by the application developer that indicates the appropriate type of service for the data in the packet. The way the bits are set determines whether the packet is queued for sending with minimum delay, maximum throughput, low cost, or mid-way "best-effort" settings depending upon the requirements of the data. The ToS field is used by the Professional Access Point to provide configuration control over *Quality of Service* (QoS) queues for data transmitted from the access point to client stations.

U

UDP

The *User Datagram Protocol* (UDP) is a transport layer protocol providing simple but unreliable datagram services. It adds port address information and a checksum to an IP packet.

UDP neither guarantees delivery nor does it require a connection. It is lightweight and efficient. All error processing and retransmission must be performed by the application program.

Unicast

A *Unicast* sends a message to a single, specified receiver. In wireless networks, unicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames directly to a single client station MAC address on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Multicast and Broadcast.

URL

A *Uniform Resource Locator* (URL) is a standard for specifying the location of objects on the Internet, such as a file or a newsgroup. URLs are used extensively in HTML documents to specify the target of a hyperlink which is often another HTML document (possibly stored on another computer). The first part of the URL indicates what protocol to use and the second part specifies the IP address or the domain name where that resource is located.

For example, `ftp://ftp.usr.com/downloads/myfile.tar.gz` specifies a file that should be fetched using the FTP protocol; `http://www.usr.com/index.html` specifies a Web page that should be fetched using the HTTP protocol.

V

VLAN

A *virtual* LAN (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth, and are isolated on that network. The Professional Access Point supports the configuration of a wireless VLAN. This technology is used on the access point for the virtual guest network feature.

VPN

A *Virtual Private Network* (VPN) is a network that uses the Internet to connect its nodes. It uses encryption and other mechanisms to ensure that only authorized users can access its nodes and that data cannot be intercepted.

W

WAN

A *Wide Area Network* (WAN) is a communications network that spans a relatively large geographical area, extending over distances greater than one kilometer. A WAN is often connected through public networks, such as the telephone system. It can also be connected through leased lines or satellites.

The Internet is essentially a very large WAN.

WDS

A *Wireless Distribution System* (WDS) allows the creation of a completely wireless infrastructure. Typically, an Access Point is connected to a wired LAN. WDS allows access points to be connected wirelessly. The access points can function as wireless repeaters or bridges.

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission.

Wi-Fi

A test and certification of interoperability for WLAN products based on the IEEE 802.11 standard promoted by the Wi-Fi Alliance, a non-profit trade organization.

WINS

The *Windows Internet Naming Service* (WINS) is a server process for resolving Windows-based computer names to IP addresses. It provides information that allows these systems to browse remote networks using the *Network Neighborhood*.

Wireless Networking Framework

There are two ways of organizing a wireless network:

- Stations communicate directly with one another in an Ad-hoc Mode network, also known as an independent basic service set (IBSS).
- Stations communicate through an Access Point in an Infrastructure Mode network. A single access point creates an infrastructure basic service set (BSS) whereas multiple access points are organized in an extended service set (ESS).

WLAN

Wireless Local Area Network (WLAN) is a LAN that uses high-frequency radio waves rather than wires to communicate between its nodes.

WMM

Wireless Multimedia (WMM) is a IEEE technology standard designed to improve the quality of audio, video and multimedia applications on a wireless network. Both access points and wireless clients (laptops, consumer electronics products) can be WMM-enabled. WMM features are based on is a subset of the WLAN IEEE 802.11e draft specification. Wireless products that are built to the standard and pass a set of quality tests can carry the "Wi-Fi certified for WMM" label to ensure interoperability with other such products. For more information, see the WMM page on the Wi-Fi Alliance Web site: http://www.wi-fi.org/OpenSection/wmm.asp.

WPA

Wi-Fi Protected Access (WPA) is a Wi-Fi Alliance version of the draft IEEE 802.11i standard. It provides more sophisticated data encryption than WEP and also provides user authentication. WPA includes TKIP and 802.1x mechanisms.

WPA2

Wi-Fi Protected Access (WPA2) is an enhanced security standard, described in IEEE 802.11i, that uses Advanced Encryption Standard (AES) for data encryption.

The original WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. WPA2 is backwards-compatible with products that support the original WPA.

WPA2, like the original WPA, supports an *Enterprise* and *Personal* version. The Enterprise version requires use of IEEE 802.1x security features and *Extensible Authentication Protocol* (EAP) authentication with a RADIUS server.

The Personal version does not require IEEE 802.1x or EAP. It uses a *Pre-Shared Key* (PSK) password to generate the keys needed for authentication.

WRAP

Wireless Robust Authentication Protocol (WRAP) is an encryption method for 802.11i that uses AES but another encryption mode (OCB) for encryption and integrity.

X

XML

The *Extensible Markup Language* (XML) is a specification developed by the W3C. XML is a simple, flexible text format derived from *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986, designed especially for electronic publishing.

Index